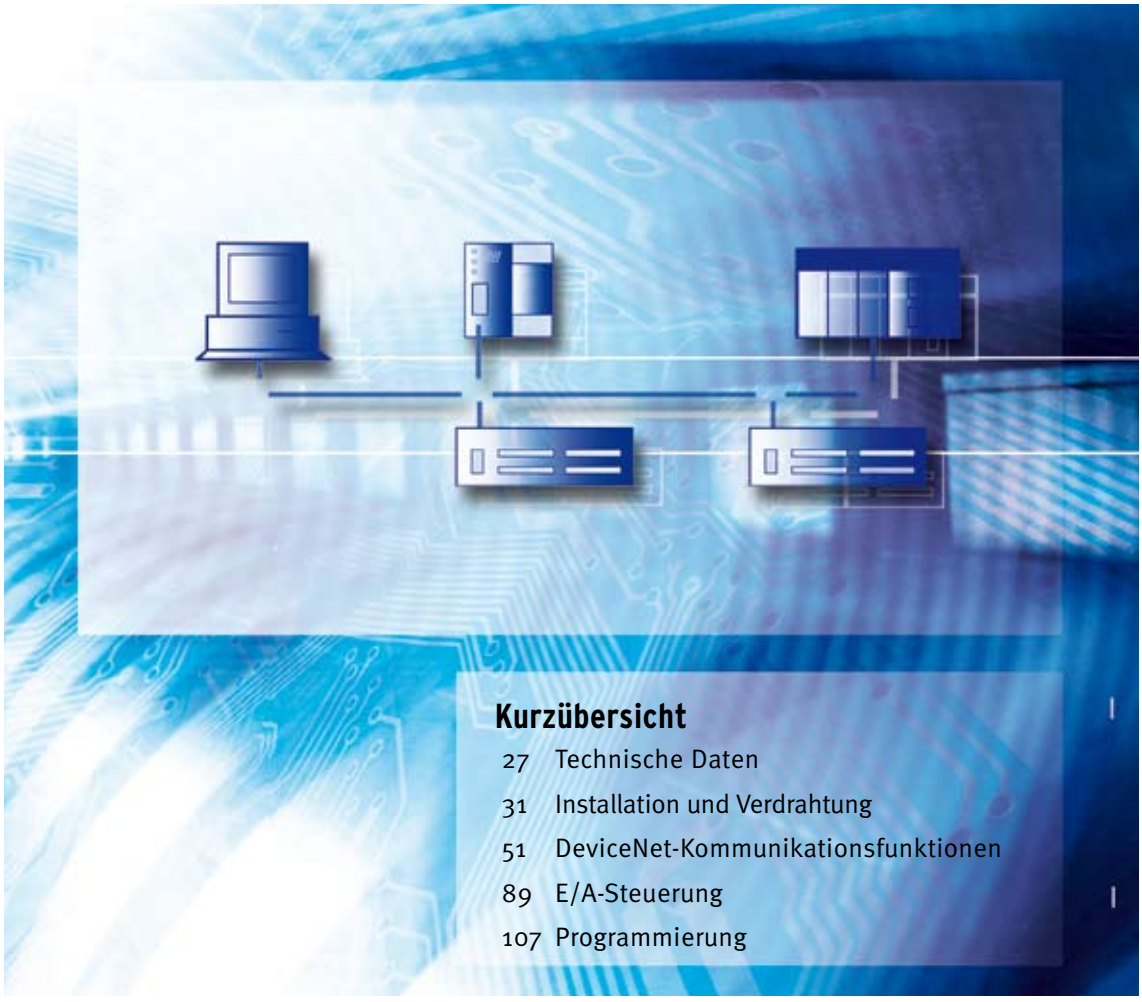
Cat. No. Z906-DE2-03

Sicherheitsnetzwerk-Controller NE1A-SCPU01(-V1)/-SCPU02

BEDIENUNGSANLEITUNG



Kurzübersicht

27 Technische Daten
31 Installation und Verdrahtung
51 DeviceNet-Kommunikationsfunktionen
89 E/A-Steuerung
107 Programmierung

Advanced Industrial Automation

OMRON

Sicherheitsnetzwerk-Controller
NE1A-SCPU01(-V1)/-SCPU02
Bedienungsanleitung

Revisionsstand September 2006

Hinweis:

OMRON-Produkte sind nur zur ordnungsgemäßen Verwendung durch qualifiziertes Personal und nur für die in diesem Handbuch beschriebenen Zwecke zugelassen.

In diesem Handbuch sind Sicherheitshinweise entsprechend der folgenden Konventionen gekennzeichnet. Beachten Sie stets die in diesen Sicherheitshinweisen enthaltenen Informationen. Ein Nichtbeachten der Sicherheitshinweise kann

zu Personen- oder Sachschäden führen.

⚠ **VORSICHT** Kennzeichnet eine potenziell gefährliche Situation, die zu leichten, mittelschweren oder schweren Verletzungen oder sogar zum Tod führen kann, wenn sie nicht vermieden wird. Außerdem können erhebliche Sachschäden verursacht werden.

Kennzeichnet allgemeine Verbote, für die es kein spezielles Symbol gibt.

Kennzeichnet unbedingt zu beachtende allgemeine Anweisungen, für die es kein spezielles Symbol gibt.

Verweise auf OMRON-Produkte

Alle Namen von OMRON-Produkten werden in diesem Handbuch großgeschrieben. Das Wort „Baugruppe“ wird ebenfalls groß geschrieben, wenn es sich auf ein OMRON-Produkt bezieht, unabhängig davon, ob es im Eigennamen des Produkts auftritt oder nicht.

Die Abkürzung „SPS“ steht für speicherprogrammierbare Steuerung. In manchen Programmierkonsolenanzeigen wird jedoch noch die Abkürzung „PC“ für „Programmable Controller“ verwendet. Dies ist nicht mit der üblichen Bedeutung von PC (z. B. Industrie-PC) zu verwechseln.

Visuelle Hilfen

Die folgenden Überschriften tauchen in der linken Spalte des Handbuchs auf und helfen Ihnen, verschiedene Arten von Informationen zu finden.

WICHTIG Kennzeichnet wichtige Informationen zu Schritten, die zur Vermeidung von Ausfällen, Fehlfunktionen und unerwünschten Auswirkungen auf die Leistung des Produkts unbedingt vorzunehmen oder unbedingt zu unterlassen sind.

Hinweis Kennzeichnet Informationen von besonderem Interesse für den effizienten und zweckmäßigen Einsatz des Produkts.

1,2,3... 1. Kennzeichnet Listen, z.B. Vorgehensweisen oder Checklisten.

Marken und Copyrights

DeviceNet und DeviceNet Safety sind eingetragene Marken der Open DeviceNet Vendors Association (ODVA).

Andere Produkt- und Firmennamen, die in diesem Handbuch erwähnt werden, sind Marken oder eingetragene Marken der jeweiligen Unternehmen.

© OMRON, 2005

Alle Rechte vorbehalten. Diese Publikation darf ohne vorherige schriftliche Genehmigung von OMRON weder als Ganzes noch in Auszügen in irgendeiner Form oder auf irgendeine Weise, sei es auf mechanischem oder elektronischem Weg oder durch Fotokopieren oder Aufzeichnen, reproduziert, in einem Datensystem gespeichert oder übertragen werden.

In Bezug auf die in dieser Publikation enthaltenen Informationen wird keine Patenthaftung übernommen. Da OMRON laufend an der Verbesserung seiner Qualitätsprodukte arbeitet, sind Änderungen an den in dieser Publikation enthaltenen Informationen ohne Ankündigung vorbehalten. Bei der Erstellung dieses Handbuchs wurden alle erdenklichen Vorsorgemaßnahmen ergriffen. Dennoch übernimmt OMRON keine Verantwortung für etwaige Fehler oder Auslassungen. Ebenso wird keine Haftung für Schäden übernommen, die aus der Nutzung der in dieser Publikation enthaltenen Informationen resultieren.

INHALTSVERZEICHNIS

SICHERHEITSHINWEISE xvii

1 Zielgruppe xviii
2 Allgemeine Sicherheitshinweise xviii
3 Sicherheitsvorkehrungen xxi
4 Hinweise zur sicheren Verwendung xxii
5 Zusätzliche Vorsichtsmaßnahmen gemäß UL 1604 xxiv
6 Richtlinien und Normen xxiv
7 Geräteversionen für Sicherheitsnetzwerk-Controller NE1A xxv

ABSCHNITT 1
Überblick: Sicherheitsnetzwerk-Controller NE1A 1

1-1 Sicherheitsnetzwerk-Controller NE1A 2
1-2 Systemkonfiguration 8
1-3 Vorgehensweise bei der Einrichtung des Systems 16

ABSCHNITT 2
Technische Daten und Bezeichnungen 17

2-1 Bezeichnungen der Komponenten, Anzeigen und Bedienelemente 18
2-2 Technische Daten 27

ABSCHNITT 3
Installation und Verdrahtung 31

3-1 Installation 32
3-2 Verdrahtung 39

ABSCHNITT 4
DeviceNet-Kommunikationsfunktionen 51

4-1 Anfangskonfiguration 52
4-2 Netzwerkstatusanzeige 55
4-3 Zuordnung dezentraler E/A-Punke 57
4-4 Sicherheits-Master-Funktion 69
4-5 Sicherheits-Slave-Funktion 75
4-6 Standard-Slave-Funktion 79
4-7 Explicit Message-Kommunikation 83

ABSCHNITT 5
E/A-Steuerung 89

5-1 Allgemeine Funktionen 90
5-2 Sicherheitseingänge 97
5-3 Testausgänge 102
5-4 Sicherheitsausgänge 103

INHALTSVERZEICHNIS

ABSCHNITT 6
Programmierung 107

6-1 Übersicht über die Programmierung 108
6-2 Funktionsblöcke – Übersicht 111
6-3 Parametrieren von Funktionsblöcken 112
6-4 Befehlsreferenz: Logikfunktionen 117
6-5 Befehlsreferenz: Funktionsblöcke 129

ABSCHNITT 7
Sonstige Funktionen 177

7-1 Konfigurationsschutz 178
7-2 Rücksetzung 179
7-3 Zugangsbeschränkung durch Kennwort 180

ABSCHNITT 8
Betriebsmodi und Verhalten bei Spannungseinbrüchen und -ausfällen 181

8-1 Betriebsmodi des Sicherheitsnetzwerk-Controllers NE1A 182
8-2 Verhalten bei Spannungseinbrüchen und -ausfällen 186

ABSCHNITT 9
Kommunikationsvermögen der dezentralen E/A und Ansprechzeit der lokalen E/A 187

9-1 Übersicht 188
9-2 Betriebsablauf und Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A 189
9-3 E/A-Aktualisierungszykluszeit und Netzwerkreaktionszeit 191
9-4 Reaktionszeit 193

ABSCHNITT 10
Fehlersuche 199

10-1 Fehlerkategorien 200
10-2 Ermittlung des Fehlerzustands 201
10-3 Anzeige-/Displaystatus und Abhilfemaßnahmen beim Auftreten von Fehlern 202
10-4 Fehlerprotokoll 207
10-5 Fehler beim Herunterladen 212
10-6 Fehler beim Zurücksetzen 215
10-7 Fehler beim Wechsel des Betriebsmodus 216
10-8 Verbindungsstatus-Tabellen 217

INHALTSVERZEICHNIS

ABSCHNITT 11
Wartung und Inspektion 223
11-1 Inspektion 224
11-2 Austausch des Sicherheitsnetzwerk-Controllers NE1A 225

Anhang 227

Glossar 253

Índice 255

Versionshistorie. 259

INHALTSVERZEICHNIS

Zu diesem Handbuch

Dieses Handbuch beschreibt Installation und Betrieb des NE1A Sicherheits-

Netzwerk-Controllers.

Lesen Sie dieses Handbuch bitte sorgfältig durch. Installieren oder betreiben Sie den NE1A nicht, bevor Sie die bereitgestellten Informationen verstanden haben. Lesen Sie unbedingt sämtliche im folgenden Abschnitt aufgeführten Vorsichtsmaßnahmen durch.

Begriffsklärung NE1A Controller

Im vorliegenden Handbuch bezeichnet der Begriff „NE1A Controller“ die Sicherheitsnetzwerk-Controller NE1A-SCPU01 und NE1A-SCPU02.

Informationen zu DeviceNet und DeviceNet Safety finden Sie in den nachstehend aufgeführten Handbüchern:

Bedienerhandbuch für den Sicherheitsnetzwerk-Controller NE1A (Z906, dieses Handbuch)

Dieses Handbuch beschreibt die technischen Daten, die Funktionen und die Anwendung der Sicherheitsnetzwerk-Controller NE1A-SCPU01 und NE1A-SCPU02.

DeviceNet Safety Systemkonfigurations-Handbuch (Z905)

Dieses Handbuch beschreibt die Konfiguration des DeviceNet Safety-Systems mithilfe des Netzwerkkonfigurators.

DeviceNet Bedienerhandbuch (W267)

Dieses Handbuch beschreibt den Aufbau und die Verbindungen in einem DeviceNet-Netzwerk. Es enthält detaillierte Informationen zur Installation und den technischen Daten der Kabel, Steckbindungen und anderer im Netzwerk eingesetzter Peripheriegeräte sowie der benötigten Spannungsversorgung. Bevor Sie versuchen, ein DeviceNet-System einzusetzen, müssen Sie dieses Handbuch sorgfältig durchgelesen und die darin enthaltenen Informationen in vollem Umfange verstanden haben.

⚠ **VORSICHT** Falls Sie die in diesem Handbuch enthaltenen Informationen nicht durchlesen oder nicht verstehen, kann dies zur Verletzung oder zum Tod von Personen oder zu einer Beschädigung oder einem Ausfall des Produkts führen. Lesen Sie jeden Abschnitt vollständig durch, und führen Sie die vorgestellten Prozeduren erst durch, wenn Sie sicher sind, dass Sie die im jeweiligen Abschnitt und den damit verbundenen Abschnitten bereitgestellten Informationen verstanden haben.

Lesen Sie dieses Handbuch sorgfältig durch

Bitte lesen Sie dieses Handbuch vor der Verwendung des Produkts sorgfältig durch. Bei Fragen oder Anmerkungen wenden Sie sich bitte an Ihre OMRON Vertretung.

Gewährleistung und Haftungsbeschränkungen

GEWÄHRLEISTUNG

OMRON gewährleistet ausschließlich, dass die Produkte frei von Material- und Produktionsfehlern sind. Diese Gewährleistung erstreckt sich (falls nicht anders angegeben) auf zwei Jahre ab Kaufdatum bei OMRON.

OMRON ÜBERNIMMT KEINERLEI GEWÄHRLEISTUNG ODER ZUSAGE, WEDER EXPLIZIT NOCH IMPLIZIT, BEZÜGLICH DER NICHTVERLETZUNG VON RECHTEN DRITTER, DER MARKTTAUGLICHKEIT ODER DER EIGNUNG DER PRODUKTE FÜR EINEN BESTIMMTEN ZWECK. JEDER KÄUFER ODER BENUTZER ERKENNT AN, DASS DER KÄUFER ODER BENUTZER ALLEINE ZU BESTIMMEN HAT, OB DIE JEWEILIGEN PRODUKTE FÜR DEN VORGESEHENEN VERWENDUNGSZWECK GEEIGNET SIND. OMRON SCHLIESST ALLE ÜBRIGEN IMPLIZITEN UND EXPLIZITEN GEWÄHRLEISTUNGEN AUS.

HAFTUNGSBESCHRÄNKUNGEN

OMRON ÜBERNIMMT KEINE VERANTWORTUNG FÜR SPEZIELLE, INDIREKTE ODER FOLGESCHÄDEN, GEWINNAUSFÄLLE ODER KOMMERZIELLE VERLUSTE, DIE IN IRGENDEINER WEISE MIT DEN PRODUKTEN IN ZUSAMMENHANG STEHEN, UNABHÄNGIG DAVON, OB SOLCHE ANSPRÜCHE AUF VERTRÄGEN, GARANTIEN, VERSCHULDUNGS- ODER GEFÄHRDUNGSHAFTUNG BASIEREN.

OMRON ist in keinem Fall haftbar für jedwede Ansprüche, die über den jeweiligen Kaufpreis des Produkts hinausgehen, für das der Haftungsanspruch geltend gemacht wird.

OMRON ÜBERNIMMT IN KEINEM FALL DIE VERANTWORTUNG FÜR GEWÄHRLEISTUNGS- ODER INSTANDSETZUNGSANSPRÜCHE IM HINBLICK AUF DIE PRODUKTE, SOWEIT DIE UNTERSUCHUNG DURCH OMRON NICHT ERGEBEN HAT, DASS DIE PRODUKTE ORDNUNGSGEMÄSS GEHANDHABT, GELAGERT, INSTALLIERT UND GEWARTET WURDEN UND KEINERLEI BEEINTRÄCHTIGUNG DURCH VERSCHMUTZUNG, MISSBRAUCH, UNSACHGEMÄSSE VERWENDUNG ODER UNSACHGEMÄSSE MODIFIKATION ODER INSTANDSETZUNG AUSGESETZT WAREN.

Anwendungshinweise

EIGNUNG

OMRON übernimmt keinerlei Verantwortung für die Einhaltung der für die konkrete Anwendung oder Kombination der Produkte (Maschinen, Anlagen usw.) geltenden Normen, Standards usw.

Auf Kundenwunsch stellt OMRON geeignete Zertifizierungsunterlagen Dritter zur Verfügung, aus denen Nennwerte und Anwendungsbeschränkungen der jeweiligen Produkte hervorgehen. Diese Informationen allein sind nicht ausreichend für die vollständige Bestimmung der Eignung der Produkte in Kombination mit Endprodukten, Maschinen, Systemen oder anderen Anwendungsbereichen.

Es folgen einige Anwendungsbeispiele, denen besondere Beachtung zu schenken ist. Es handelt sich nicht um eine umfassende Liste aller Verwendungsmöglichkeiten der Produkte. Diese Liste ist auch nicht so zu verstehen, dass die Produkte für die angegebenen Verwendungsmöglichkeiten geeignet sind.

- Verwendung im Freien, Verwendung mit potenziellen chemischen Verunreinigungen oder unter elektrischer Beeinflussung oder unter Bedingungen oder Verwendungen, die nicht in diesem Handbuch beschrieben werden.
- Nukleartechnik, Verbrennungsanlagen, Schienenverkehr, Luftfahrt, Medizintechnik, Spielautomaten, Sicherheitseinrichtungen und andere Anlagen, die speziellen industriellen und/oder behördlichen Anforderungen und Auflagen unterliegen.
- Systeme, Maschinen und Geräte, die eine Gefahr für Leben und Eigentum darstellen können.

Machen Sie sich bitte mit allen Einschränkungen im Hinblick auf die Verwendung dieser Produkte vertraut, und halten Sie diese ein.

VERWENDEN SIE DAS PRODUKT NIEMALS FÜR ANWENDUNGEN, DIE EINE GEFAHR FÜR LEBEN ODER EIGENTUM DARSTELLEN, OHNE SICHERZUSTELLEN, DASS DAS GESAMTSYSTEM UNTER BERÜCKSICHTIGUNG DER JEWEILIGEN RISIKEN KONZIPIERT UND DAS OMRON PRODUKT HINSICHTLICH DER BEABSICHTIGTEN VERWENDUNG IN DER GESAMTANLAGE BZW. DES GESAMTSYSTEMS ORDNUNGSGEMÄSS EINGESTUFT UND INSTALLIERT WIRD.

PROGRAMMIERBARE PRODUKTE

OMRON übernimmt keine Verantwortung für die Programmierung eines programmierbaren Produkts durch den Benutzer und die daraus resultierenden Konsequenzen.

Haftungsausschlüsse

ÄNDERUNG DER TECHNISCHEN DATEN

Im Zuge der technischen Weiterentwicklung und aus anderen Gründen können jederzeit Änderungen an den technischen Daten und den verfügbaren Zubehörteilen des Produkts erfolgen.

Üblicherweise ändern wir die Modellnummern, wenn veröffentlichte Nennwerte oder Funktionen geändert oder signifikante Konstruktionsänderungen vorgenommen werden. Manche technischen Daten der Produkte werden möglicherweise ohne Mitteilung geändert. Im Zweifelsfall können auf Anfrage spezielle Modellnummern zugewiesen werden, um für Ihre Anwendung wesentliche technische Daten zu fixieren. Bei Fragen zu technischen Daten erworbener Produkte können Sie sich jederzeit an den OMRON Vertrieb wenden.

ABMESSUNGEN UND GEWICHT

Die Angaben zu Abmessungen und Gewicht sind Nennwerte, die nicht für Fertigungszwecke bestimmt sind, auch wenn Toleranzen angegeben sind.

LEISTUNGSDATEN

Die in diesem Handbuch genannten Leistungsdaten dienen als Anhaltspunkt zur Beurteilung der Eignung durch den Benutzer und werden nicht garantiert. Die Daten können auf Testbedingungen von OMRON basieren und müssen vom Benutzer auf die tatsächliche Anwendungssituation übertragen werden. Die tatsächliche Leistung unterliegt der Garantie und Haftungsbeschränkung von OMRON.

FEHLER UND AUSLASSUNGEN

Die in diesem Handbuch enthaltenen Informationen wurden sorgfältig geprüft und sind unserer Ansicht nach korrekt. OMRON übernimmt jedoch keine Verantwortung für evtl. trotz sorgfältiger Durchsicht verbliebene Tipp- oder Schreibfehler oder Auslassungen.

SICHERHEITSHINWEISE

1 Zielgruppe xviii
2 Allgemeine Sicherheitshinweise xviii
3 Sicherheitsvorkehrungen xxi
4 Hinweise zur sicheren Verwendung xxii
5 Zusätzliche Vorsichtsmaßnahmen gemäß UL 1604 xxiv
6 Richtlinien und Normen xxiv
7 Geräteversionen für Sicherheitsnetzwerk-Controller NE1A xxv

1 Zielgruppe

Dieses Handbuch richtet sich an folgende Personen, die sich mit elektrischen Anlagen auskennen müssen (z. B. Elektrotechniker und -ingenieure):

- Das für die Einrichtung von Automatisierungs- und Sicherheitssystemen in Produktionsstätten zuständige Personal
- Das für die Konstruktion von Automatisierungs- und Sicherheitssystemen zuständige Personal
- Das für die Verwaltung von Automatisierungs-Systemen zuständige Personal
- Das aufgrund seiner Qualifikation, Autorität und Verantwortlichkeit für die Gewährleistung der Sicherheit in den Produktphasen „Mechanischer Entwurf“, „Installation“, „Betrieb“, „Wartung“ und „Entsorgung“ zuständige Personal.

2 Allgemeine Sicherheitshinweise

Der Benutzer muss das Produkt gemäß den in den Bedienerhandbüchern beschriebenen Leistungsspezifikationen betreiben.

Wenden Sie sich vor der Verwendung dieses Produkts an den OMRON Vertrieb, wenn Sie das Produkt unter Bedingungen einsetzen, die nicht im Handbuch aufgeführt sind bzw. wenn Sie das Produkt im Bereich der Nukleartechnik, im Eisenbahnverkehr, in der Luftfahrt, in Fahrzeugen, in Verbrennungssystemen, in medizinischen Geräten, in Spielautomaten, in Sicherheitsausrüstungen oder anderen Systemen, Geräten oder Ausrüstungen verwenden möchten, bei denen bei fehlerhafter Verwendung die Gefahr von Personen- oder Sachschäden besteht.

Achten Sie darauf, dass die Nenn- und Leistungsdaten des Produkts für die jeweiligen Systeme, Maschinen und Anlagen angemessen sind, und statten Sie die Systeme, Maschinen und Anlagen mit redundanten Sicherheitsmechanismen aus.

Dieses Handbuch enthält Informationen zu Programmierung und Betrieb des Produkts. Lesen Sie dieses Handbuch vor Verwendung des Produkts durch, und halten Sie dieses Handbuch während des Betriebs zu Referenzzwecken immer griffbereit.

⚠ VORSICHT Es ist außerordentlich wichtig, dass SPS und alle SPS-Baugruppen nur für den vorgegebenen Einsatzzweck und unter den angegebenen Bedingungen verwendet werden. Dies gilt besonders für Anwendungen, bei denen direkt oder indirekt die Gefahr von Personenschäden besteht. Wenden Sie sich an den OMRON Vertrieb, bevor Sie ein SPS-System für die oben aufgeführten Anwendungen einsetzen.

⚠ VORSICHT Dies ist das Bedienerhandbuch für die Sicherheitsnetzwerk-Controller NE1A. Berücksichtigen Sie bei der Konstruktion des Systems die folgenden Aspekte, um sicherzustellen, dass die sicherheitsrelevanten Komponenten so konfiguriert werden, dass ein sicherer Betrieb der Systemfunktionen möglich ist.

• Risikobeurteilung

Die in diesem Bedienerhandbuch beschriebene ordnungsgemäße Anwendung der Sicherheitseinrichtungen in Hinsicht auf die Installationsbedingungen und die mechanischen Leistungsdaten und Funktionen muss unbedingt eingehalten werden. Bei der Auswahl und Anwendung dieser Sicherheitseinrichtung muss bereits bei der Entwicklung der Anlage oder

Installation eine Risikobeurteilung durchgeführt werden, um mögliche gefährdende Faktoren der Anlage oder Installation, in der die Sicherheitseinrichtung eingesetzt wird, zu identifizieren. Die Auswahl geeigneter Sicherheitseinrichtungen muss unter der Anleitung eines hinreichenden Risikobeurteilungssystems erfolgen. Ein unzureichendes Risikobeurteilungssystem kann zur Auswahl ungeeigneter Sicherheitseinrichtungen führen.

- Entsprechende internationale Normen (Auswahl): ISO 14121: Sicherheit von Maschinen – Leitsätze zur Risikobeurteilung

- **Sicherheitsvorkehrungen**

  Die Anwendung dieser Sicherheitseinrichtung für die Konstruktion von Systemen mit sicherheitsrelevanten Komponenten für Anlagen oder Installationen muss in völliger Übereinstimmung mit internationalen Normen wie den im Folgenden aufgeführten und/oder den Normen der jeweiligen Industrie erfolgen.

  - Entsprechende internationale Normen (Auswahl): ISO/DIS 12100: Sicherheit von Maschinen – Grundbegriffe, Allgemeine Gestaltungsleitsätze; IEC 61508: Sicherheitsnorm für sicherheitsbezogene Systeme (Funktionale Sicherheit von elektrischen/elektronischen/programmierbaren Sicherheitssystemen)

- **Die Rolle der Sicherheitseinrichtung**

  Diese Sicherheitseinrichtung ist mit den in den relevanten Normen festgelegten Sicherheitsfunktionen und -mechanismen ausgestattet. Durch geeignete Konstruktion muss jedoch sichergestellt werden, dass diese Funktionen und Mechanismen im Rahmen der Systemkonstruktion mit sicherheitsrelevanten Komponenten ordnungsgemäß operieren. Ein umfassendes Verständnis um das Funktionsprinzip dieser Funktionen und Mechanismen ist für die Konstruktion von Systemen, die diese ordnungsgemäß anwenden, unerlässlich.

  - Entsprechende internationale Normen (Auswahl): ISO 14119: Sicherheit von Maschinen – Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl

- **Installation der Sicherheitseinrichtung**

  Die Konstruktion und Installation von Systemen mit sicherheitsrelevanten Komponenten für Anlagen und Installationen muss durch entsprechend geschulte Techniker erfolgen.

  - Entsprechende internationale Normen (Auswahl): ISO/DIS 12100: Sicherheit von Maschinen – Grundbegriffe, Allgemeine Gestaltungsleitsätze; IEC 61508: Sicherheitsnorm für sicherheitsbezogene Systeme (Funktionale Sicherheit von elektrischen/elektronischen/programmierbaren Sicherheitssystemen)

- **Übereinstimmung mit Gesetzen und Richtlinien**

  Diese Sicherheitseinrichtung entspricht den relevanten Richtlinien und Normen, jedoch muss sichergestellt werden, dass sie in Übereinstimmung mit den für die jeweilige Anlage oder Installation geltenden lokalen Richtlinien und Normen eingesetzt wird.

  - Entsprechende internationale Normen (Auswahl): EN 60204: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen

- **Beachtung der Anwendungshinweise**

  Beim konkreten Einsatz der ausgewählten Sicherheitseinrichtung müssen die in diesem Bedienerhandbuch und in dem der Sicherheitseinrichtung beiliegenden Bedienerhandbuch aufgeführten technischen Daten und Vorsichtsmaßnahmen beachtet werden. Der Einsatz des Produkts auf eine im Widerspruch zu diesen technischen Daten und Vorsichtsmaßnahmen stehende Art und Weise kann aufgrund unzureichender Betriebsfunktionen der sicherheitsrelevanten Komponenten zu unerwarteten Ausfällen der Anlagen und Geräte und zu entsprechenden aus solchen Ausfällen resultierenden Schäden führen.

- **Verlagerung oder Weiterveräußerung von Geräten und Anlagen**

  Bei Versand oder Weiterveräußerung von Geräten und Anlagen sind die entsprechenden Dokumentationen wie beispielsweise dieses Bedienerhandbuch ebenfalls an den Empfänger weiterzugeben, um diesem den ordnungsgemäßen Betrieb zu ermöglichen.

  - Entsprechende internationale Normen (Auswahl): ISO/DIS 12100: Sicherheit von Maschinen – Grundbegriffe, Allgemeine Gestaltungsleitsätze IEC 61508: Sicherheitsnorm für sicherheitsbezogene Systeme (Funktionale Sicherheit von elektrischen/elektronischen/programmierbaren Sicherheitssystemen)

3 Sicherheitsvorkehrungen

⚠ VORSICHT	
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, dürfen die Testausgänge des Sicherheitsnetzwerk-Controllers NE1A nicht als Sicherheitsausgänge benutzt werden.	
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, dürfen DeviceNet-Standard-E/A-Daten oder Explicit-Message-Daten nicht als Sicherheitssignale verwendet werden.	
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, dürfen die Anzeigen des Sicherheitsnetzwerk-Controllers NE1A nicht für Sicherheitsfunktionen verwendet werden.	
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, dürfen keine Lasten an die Sicherheits- oder Testausgänge angeschlossen werden, die den Nennwert übersteigen.	
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, müssen die Leitungen des Sicherheitsnetzwerk-Controllers NE1A so geführt werden, dass die 24-V-DC-Leitung nicht versehentlich in Kontakt mit den Ausgängen gerät.	
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, muss der 0-V-Ausgang der Spannungsversorgung für die externen Ausgangsgeräte geerdet werden, um zu verhindern, dass die Geräte bei einem Masseschluss einer Sicherheits- oder Testausgangsleitung aktiviert werden.	
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, müssen alte Konfigurationsdaten vor dem Anschluss eines Geräts an das Netzwerk gelöscht werden.	
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, müssen vor dem Anschluss eines Geräts an das Netzwerk die Knotenadresse und die Baudrate eingestellt werden.	
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, muss vor Inbetriebnahme des Systems ein Anwendertest durchgeführt werden, um die Korrektheit der Konfigurationsdaten aller Geräte und deren ordnungsgemäße Funktion sicherzustellen.	
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, muss beim Austausch von Geräten darauf geachtet werden, dass das Austauschgerät ordnungsgemäß konfiguriert ist und einwandfrei funktioniert.	
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, müssen bei der Auswahl von Komponenten und Geräten die in der folgenden Tabelle aufgeführten Anforderungen Berücksichtigung finden.	

Steuerungsgerät	Anforderungen
NOT-AUS-Taster	Verwenden Sie zugelassene Schaltgeräte mit Zwangsöffnungsmechanismus gemäß IEC/EN 60947-5-1.
Verriegelungs- oder Positionsschalter für Sicherheitstüren	Verwenden Sie zugelassene Schaltgeräte mit Zwangsöffnungsmechanismus gemäß IEC/EN 60947-5-1, die Mikrolasten von 4 mA bei 24 V DC schalten können.
Sicherheitssensoren	Verwenden Sie zugelassene Schaltgeräte, die die Anforderungen der einschlägigen Produktstandards, Vorschriften und Gesetze im entsprechenden Land erfüllen.

Steuerungsgerät	Anforderungen
Sicherheitsrelais mit zwangsgeführten Kontakten	Verwenden Sie zugelassene Schaltgeräte mit zwangsgeführten Kontakten, die EN 50205 entsprechen. Für Rückführsignale müssen Schaltgeräte mit Kontakten verwendet werden, die Mikrolasten von 4 mA bei 24 V DC schalten können.
Schütz	Verwenden Sie Schütze mit zwangsgeführten Kontakten, und überwachen Sie den Hilfsöffnerkontakt, um Ausfälle von Schützen erkennen zu können. Für Rückführsignale müssen Schaltgeräte mit Kontakten verwendet werden, die Mikrolasten von 4 mA bei 24 VDC schalten können.
Andere Geräte	Prüfen Sie, ob die verwendeten Geräte den Anforderungen der Steuerungskategorie entsprechen.

4 Hinweise zur sicheren Verwendung

■ Handhabung

Lassen Sie den Sicherheitsnetzwerk-Controller NE1A nicht fallen, und setzen Sie ihn keinen starken Stößen oder Vibrationen aus. Andernfalls besteht die Gefahr von Fehlfunktionen.

■ Installation und Lagerung

Lagern oder installieren Sie den Sicherheitsnetzwerk-Controller NE1A nicht an den folgenden Orten:

- Orte, die dem Einfluss direkter Sonneneinstrahlung ausgesetzt sind.
- Orte, an denen Temperaturen oder Luftfeuchtigkeit außerhalb der in den technischen Daten angegebenen Bereiche herrschen.
- Orte, die starken Temperaturschwankungen und damit Kondensation ausgesetzt sind.
- Orte, die dem Einfluss korrosiver oder entzündlicher Gase ausgesetzt sind.
- Orte, die dem Einfluss von Stäuben (besonders Eisenstaub) oder Salzen ausgesetzt sind.
- Orte, die dem Einfluss von Wasser, Öl oder Chemikalien ausgesetzt sind.
- Orte, die Stößen oder Schwingungen ausgesetzt sind.

Ergreifen Sie bei der Installation von Systemen an folgenden Orten angemessene und geeignete Maßnahmen. Unangemessene oder unzureichende Maßnahmen können zu Fehlfunktionen führen.

- Orte mit statischer Aufladung und anderen Störungen.
- Orte, an denen starke elektromagnetische Felder auftreten.
- Orte, die dem Einfluss von Radioaktivität ausgesetzt sein könnten.
- Orte in der Nähe von Spannungsversorgungen.

■ Montage

- Installieren Sie den Sicherheitsnetzwerk-Controller NE1A in einen Schaltschrank mit einer Schutzklasse von mindestens IP54 (EN60529).
- Verwenden Sie für die Installation des Sicherheitsnetzwerk-Controllers NE1A im Schaltschrank eine DIN-Schiene (TH35-7,5/TH35-15 gemäß IEC 60715). Montieren Sie den Sicherheitsnetzwerk-Controller NE1A mit Hilfe von PFP-M-Abschlussstücken (nicht im Lieferumfang enthalten) auf die DIN-Schiene, um sicherzustellen, dass der Sicherheitsnetzwerk-Controller bei Vibrationen nicht von der DIN-Schiene fällt.
- Lassen Sie bei der Installation des Sicherheitsnetzwerk-Controllers NE1A für Wärmeabfuhr und Verdrahtung einen Freiraum von mindestens 5 mm (Seiten) bzw. 50 mm (oben und unten).

■ Installation und Verdrahtung

- Drähte/Litzen für den Anschluss externer E/A-Geräte an den Sicherheitsnetzwerk-Controller NE1A müssen den in der folgenden Tabelle aufgeführten Spezifikationen genügen.

Volldraht	0,2 bis 2,5 mm^2 (AWG 24 bis AWG 12)
Litze	0,34 bis 1,5 mm^2 (AWG 22 bis AWG 16) Litzen müssen vor Verwendung mit Aderendhülsen mit isolierendem Plastikkragen nach DIN 46228-4 versehen werden.

- Vor allen Verdrahtungsarbeiten muss die Spannungsversorgung ausgeschaltet werden, da andernfalls die Gefahr einer unerwarteten Aktivierung der an den Sicherheitsnetzwerk-Controller angeschlossenen Geräte besteht.
- An den Eingängen des Sicherheitsnetzwerk-Controllers NE1A dürfen nur die spezifizierten Eingangsspannungen angelegt werden. Das Anlegen einer falschen Gleichspannung oder einer beliebigen Wechselspannung kann zum Ausfall des Sicherheitsnetzwerk-Controllers NE1A führen.
- Halten Sie Leitungen für Kommunikations- und E/A-Signale getrennt von Strom- oder Hochspannungsleitungen.
- Achten Sie beim Herstellen von Verbindungen an den Anschlüssen des Sicherheitsnetzwerk-Controllers NE1A darauf, Ihre Finger nicht einzuklemmen.
- Ziehen Sie den DeviceNet-Stecker mit dem vorgesehenen Drehmoment (0,25 bis 0,3 Nm) fest.
- Eine fehlerhafte Verdrahtung kann zu einer Beeinträchtigung der Sicherheitsfunktionen führen. Führen Sie alle Verdrahtungsarbeiten ordnungsgemäß durch, und kontrollieren Sie vor der Verwendung des Sicherheitsnetzwerk-Controllers NE1A die Funktion der Verdrahtung.
- Entfernen Sie nach Abschluss der Verdrahtungsarbeiten die Staubschutzfolie, um eine ordnungsgemäße Wärmeableitung zu gewährleisten.

■ Auswahl der Spannungsversorgung

Verwenden Sie eine Gleichspannungsversorgung, die die nachstehenden Anforderungen erfüllt:

- Die Gleichspannungsversorgung verwendet eine Schutzisolierung oder verstärkte Isolierung zwischen Primär- und Sekundärkreis.
- Die Gleichspannungsversorgung muss die Anforderungen für Stromkreise der Klasse 2 oder Stromkreise mit begrenzten Spannungs-/Stromwerten gemäß UL 508 erfüllen.
- Bei einem Ausfall der Versorgungsspannung muss die Ausgangsspannung für mindestens 20 ms gehalten werden.

■ Periodische Inspektion und Wartung

- Schalten Sie vor einem Austausch des Sicherheitsnetzwerk-Controllers NE1A die Spannungsversorgung aus, da andernfalls die Gefahr einer unerwarteten Deaktivierung der an den an den Sicherheitsnetzwerk-Controller NE1A angeschlossenen Geräte besteht.
- Nehmen Sie den Sicherheitsnetzwerk-Controller NE1A nicht auseinander, und versuchen Sie nicht, ihn zu reparieren oder zu modifizieren, Bei Wiederhandlung besteht die Gefahr einer Beeinträchtigung der Sicherheitsfunktionen.

■ Entsorgung

- Gehen Sie bei der Zerlegung des Sicherheitsnetzwerk-Controllers NE1A-series vorsichtig vor, um Verletzungen zu vermeiden.

5 Zusätzliche Vorsichtsmaßnahmen gemäß UL 1604

Der Sicherheitsnetzwerk-Controller NE1A eignet sich für den Einsatz in Klasse I, Abschnitt 2, Gruppe A, B, C, D oder ausschließlich gefährdungsfreie Bereiche.

VORSICHT – Explosionsgefahr – Bei einem Austausch von Komponenten kann die Zulassung für den Betrieb in Klasse I, Abschnitt 2 erlöschen.

VORSICHT – Explosionsgefahr – Das Lösen von Verbindungen ist nur zulässig, wenn die Versorgungsspannung zuvor ausgeschaltet wurde oder nachweislich keine Explosionsgefahr im Bereich besteht.

VORSICHT – Explosionsgefahr – Das Lösen des USB-Steckers ist nur zulässig, wenn die Versorgungsspannung zuvor ausgeschaltet wurde oder nachweislich keine Explosionsgefahr im Bereich besteht.

6 Richtlinien und Normen

Der Sicherheitsnetzwerk-Controller NE1A-SCPU01 wurde wie folgt geprüft:

Prüfinstitut	Normen
TÜV Rheinland	EN954-1:1996, EN60204-1:1997, EN61000-6-2:2001, EN61000-6-4:2001, EN418:1992, IEC61508 Teil 1-7/12.98-05.00, IEC61131-2:2003,NFPA 79-2002, ANSI RIA15.06-1999, ANSI B11.19-2003
UL	UL1998, UL508, UL1604, NFPA79, IEC61508, CSA22.2 No142, CSA22.2 No213

Im Juli 2006 wurden folgende Zertifizierungen für NE1A-SCPU01-V1 und NE1A-SCPU02 beantragt, die weiterhin anhängig sind.

Prüfinstitut	Normen
TÜV Rheinland	EN954-1:1996, EN60204-1:1997, EN61000-6-2:2001, EN61000-6-4:2001, EN418:1992, IEC61508 Teil 1-7/12.98-05.00, IEC61131-2:2003,NFPA 79-2002, ANSI RIA15.06-1999, ANSI B11.19-2003
UL	UL1998, UL508, UL1604, NFPA79, IEC61508, CSA22.2 No142, CSA22.2 No213

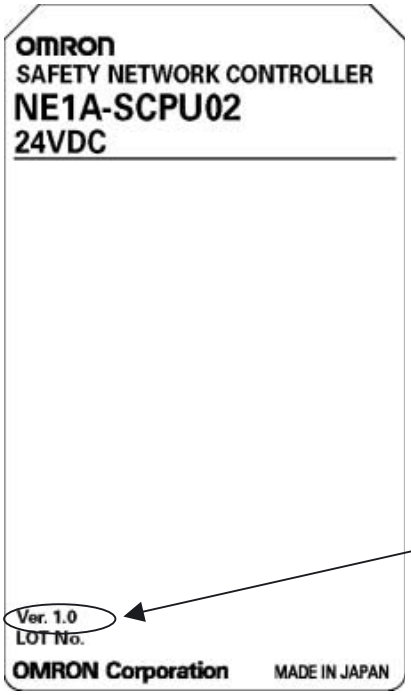
7 Geräteversionen für Sicherheitsnetzwerk-Controller NE1A

Geräteversionen

Für die Sicherheitsnetzwerk-Controller NEA1 wurde eine Geräteversion eingeführt, die Funktionsunterschiede aufgrund von Aktualisierungen berücksichtigt.

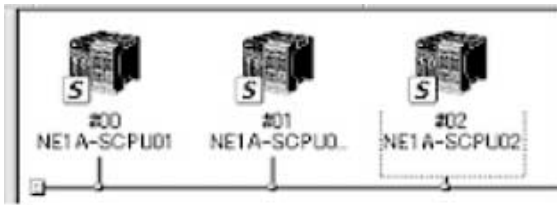
1. Angabe der Geräteversion auf dem Produkt
   Die Geräteversion (Ver. □.□) steht neben der Chargennummer auf dem Typschild, sofern eine Versionsnummer vergeben wurde.
   - Controller ohne Versionsnummer auf dem Typschild werden 1.0-Vorversions-Controller genannt.

   Typschild

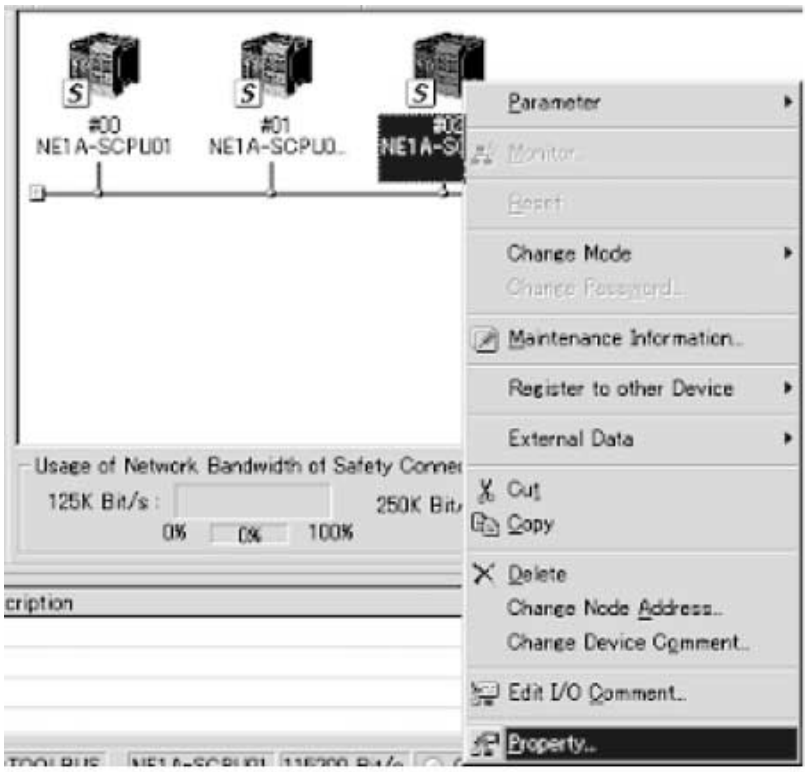


Hier steht die Geräteversion.
(Beispiel: Ver. 1.0)

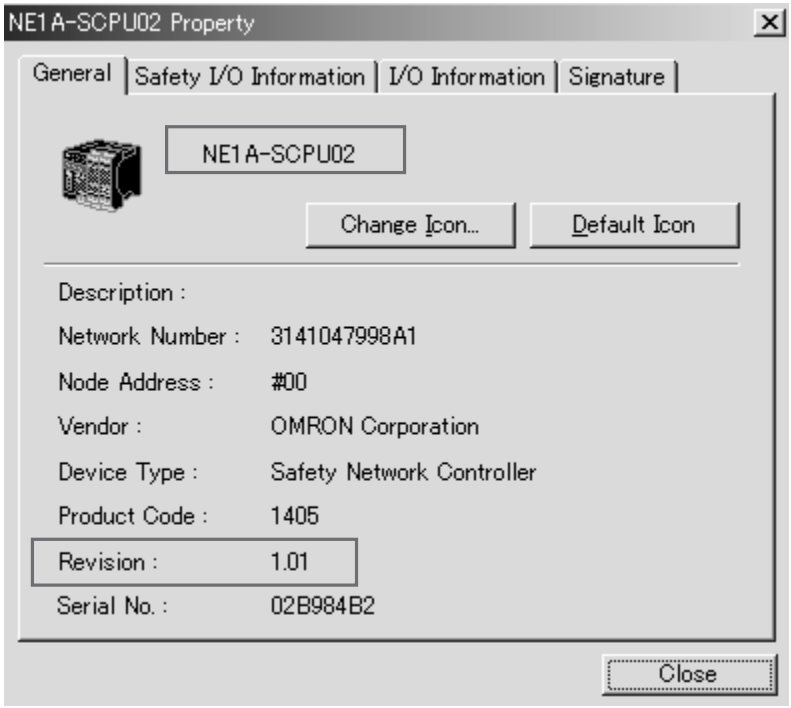
2. Überprüfung der Geräteversion mittels Supportsoftware
   Die Geräteversion kann wie folgt mit dem Netzwerkkonfigurator ab Version 1.6 geprüft werden.
   a. Laden Sie Konfigurationsdaten aus dem System hoch. Darauf werden die Gerätesymbole angezeigt (siehe nachstehende Abbildung).



   b. Klicken Sie mit der rechten Maustaste auf das Controller-Symbol, um das nachstehend abgebildete Popup-Menü anzuzeigen.
   Wählen Sie den Menüeintrag „Property“ (Eigenschaften) aus.



c. Darauf hin öffnet sich das Fenster mit den Eigenschaften des Controllers.



Das Eigenschaftenfenster enthält die Gerätebezeichnung und -revision. Die von Version 1.6□ unterstützten Sicherheitsnetzwerk-Controller der Serie NE1A sind in der nachstehenden Tabelle aufgeführt.

Modell	Gerätebezeichnung	Revision	Geräteversion
NE1A-SCPU01	NE1A-SCPU01	1.01	1.0-Vorversion
NE1A-SCPU01-V1	NE1A-SCPU01-V1	1.01	1.0
NE1A-SCPU02	NE1A-SCPU02	1.01	1.0

3. Überprüfung der Geräteversion mittels Versionsaufkleber

Folgende Versionsaufkleber sind im Lieferumfang des Controllers enthalten.

Ver. 1.0
Ver.
Ver. 1.0
Ver.
バージョンアップによるユニットの搭載機能の差異を管理するためのラベルです。
必要に応じて、製品の前面に貼り付けてご使用ください。
These labels can be used to manage differences in the available functions among the Units.
Place the appropriate label on the front of the Unit to show what Unit version is actually being used.

Diese Aufkleber können auf der Vorderseite älterer Controller aufgebracht werden, um zwischen Geräten mit unterschiedlichen Versionen zu unterscheiden.

Unterstützte Funktionen nach Geräteversion

Modell	**NE1A-SCPU01**	**NE1A-SCPU01-V1**	**NE1A-SCPU02**
Geräteversion **Funktion**	**1.0-Vorversion**	**Version 1.0**	**Version 1.0**
Logik-Operationen			
Maximale Programmgröße (Funktionsblöcke insgesamt)	128	254	254
Zusatz-Funktionsblöcke • RS Flip-flop • Multi Connector • Muting • Zustimmschalter • Impulsgeber • Zähler • Komparator	---	Unterstützt	Unterstützt
Auswahl der steigenden Flanke des Rücksetzens für die Funktionsblöcke „Reset“ und „Restart“	---	Unterstützt	Unterstützt
Nutzung des Zustands der lokalen E/A bei der Logik-Programmierung	---	Unterstützt	Unterstützt
Nutzung des allgemeinen Gerätezustands bei der Logik-Programmierung	---	Unterstützt	Unterstützt
E/A-Steuerungsfunktionen			
Schalthäufigkeitszähler	---	Unterstützt	Unterstützt
Gesamteinschaltdauer-Überwachung	---	Unterstützt	Unterstützt
DeviceNet-Kommunikationsfunktionen			
Anzahl Sicherheits-E/A-Verbindungen am Sicherheits-Master	16	32	32
Funktionsauswahl für Sicherheits-E/A-Kommunikation nach einem Kommunikationsfehler	---	Unterstützt	Unterstützt
Zusätzliche lokale Ausgangsüberwachung zwecks Datenübertragung im Slave-Betrieb	---	Unterstützt	Unterstützt
Zusätzliche lokale Eingangsüberwachung zwecks Datenübertragung im Slave-Betrieb	---	Unterstützt	Unterstützt
Systemstart und Unterstützung für das Wiederaufsetzen nach Fehlern			
Speichern der Historie geringfügiger Fehler im nichtflüchtigen Speicher	---	Unterstützt	Unterstützt
Hinzufügen von Funktionsblockfehlern zur Fehlerhistorie	---	Unterstützt	Unterstützt

Geräteversionen und Programmiergeräte

Bei Verwendung eines Sicherheitsnetzwerk-Controllers mit der Geräteversion 1.0 muss ein Netzwerkkonfigurator ab Version 1.6 verwendet werden. Die nachstehenden Tabellen verdeutlichen das Verhältnis von der Geräteversion zur Version des Netzwerkkonfigurators.

Produktbezeichnung	Netzwerkkonfigurator		
	Ver. 1.3□	**Ver. 1.5□**	**Ver. 1.6□**
NE1A-SCPU01 1.0-Vorversion	Verwendbar	Verwendbar	Verwendbar
NE1A-SCPU01-V1 mit Geräteversion 1.0	Nicht verwendbar	Nicht verwendbar	Verwendbar
NE1A-SCPU02 mit Geräteversion 1.0	Nicht verwendbar	Nicht verwendbar	Verwendbar

Upgrade für Sicherheitsnetzwerk-Controller NE1A

Das Funktionsspektrum der Modelle NE1A-SCPU01-V1 und NE1A-SCPU02 wurde gegenüber der Ausführung NE1A-SCPU01 mehrfach erweitert. Beim Wechsel von NE1A-SCPU01 zu NE1A-SCPU01-V1 oder NE1A-SCPU02 bleiben die alten Konfigurationsdaten weiterhin nutzbar, indem sie entsprechend konvertiert werden.

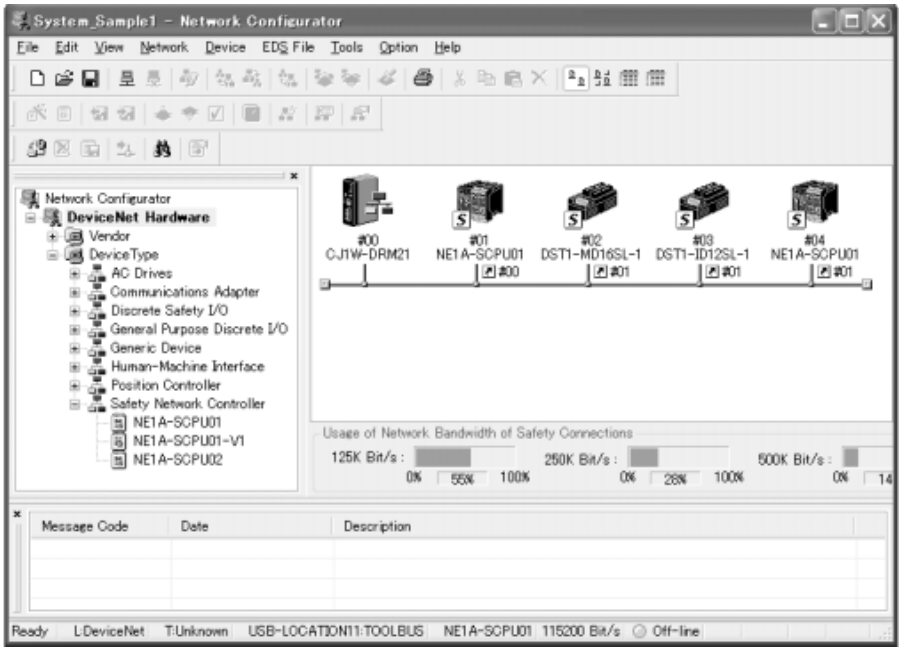
Gehen Sie wie folgt vor, um Konfigurationsdaten für die Modelle NE1A-SCPU01-V1 oder NE1A-SCPU02 aus Konfigurationsdaten für die Ausführung NE1A-SCPU01 zu generieren.

1. Lesen von Konfigurationsdaten

Gehen Sie wie folgt vor, um die Konfigurationsdaten mit dem Netzwerkkonfigurator (Version 1.6) zu lesen.

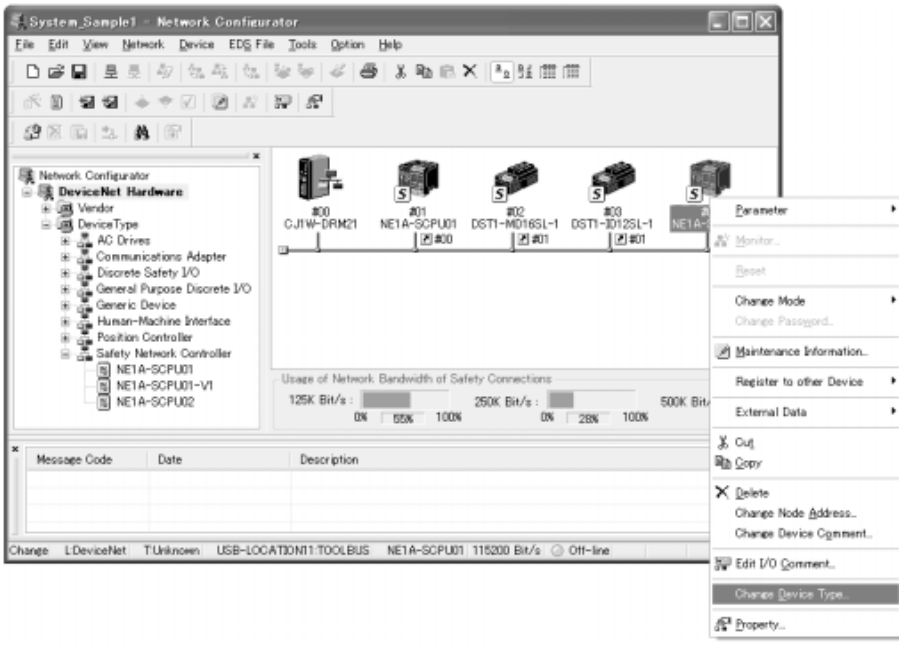
- Lesen Sie die gespeicherten Konfigurationsdaten.
- Laden Sie die Konfigurationsdaten von Geräten, die an das Netzwerk angeschlossen sind, über das Netzwerk hoch.

Nach dem Lesen der Daten wird der folgende Bildschirm angezeigt.

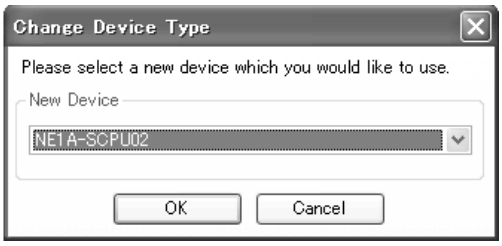


2. Konvertieren von Konfigurationsdaten

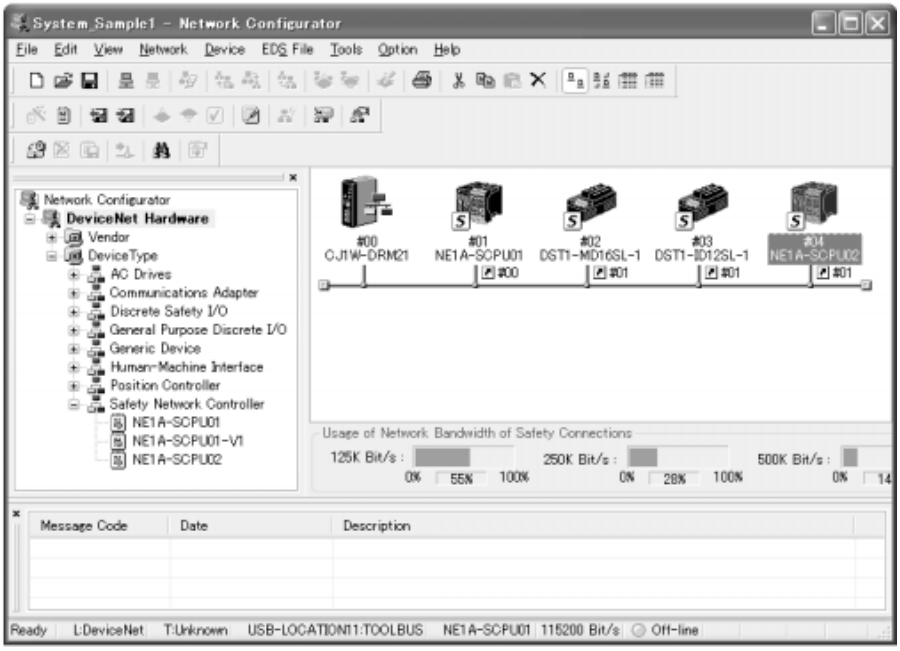
Klicken Sie in den mit dem Netzwerkkonfigurator ausgelesenen Daten auf das Gerät des Typs NE1A-SCPU01, aus dem ein Gerät des Typs NE1A-SCPU01-V1 oder NE1A-SCPU02 werden soll, und wählen Sie im Popup-Menü den Eintrag ***Change Device Type*** (Gerätetyp ändern).



Wählen Sie danach unter „New Device“ (neues Gerät) das neue Gerät aus, und drücken Sie die Schaltfläche OK.



Darauf hin ändert sich die Produktbezeichnung, und die Konfigurationsdaten für das neue Gerät werden vervollständigt.

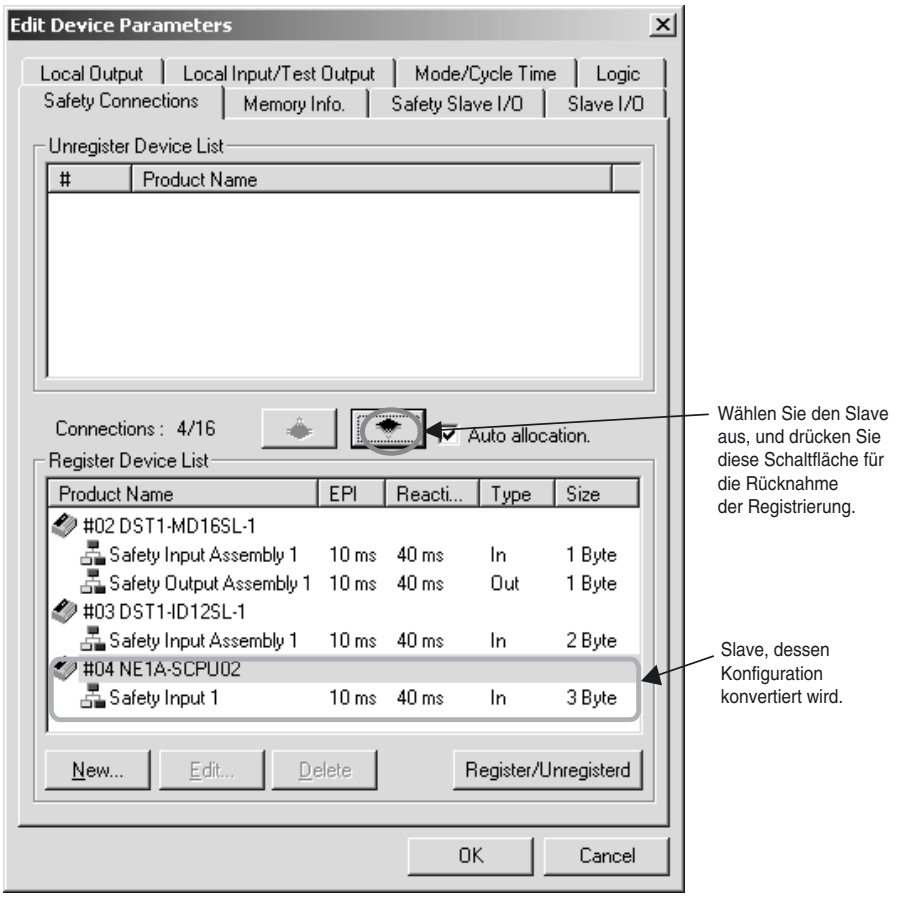


3. Erweiterungskonfiguration

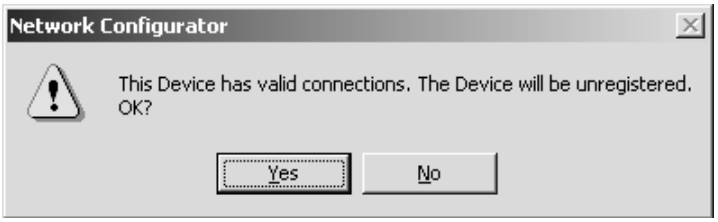
Bei der Konvertierung der Konfigurationsdaten werden alle Erweiterungsfunktionen auf ihre Standardwerte gesetzt. Konfigurieren Sie alle Erweiterungsfunktionen, die verwendet werden sollen.

4. Neuregistrierung von Sicherheits-Slaves im Sicherheits-Master

Wenn es sich bei dem Gerät, für das die Konfigurationsdaten konvertiert wurden, um einen Sicherheits-Slave handelt, muss dieser neu im Sicherheits-Master registriert werden. Wählen Sie zunächst den Slave auf der Registerkarte „Safety Connections“ (Sicherheitsverbindungen) des Sicherheits-Masters aus, und nehmen Sie die Registrierung zurück.



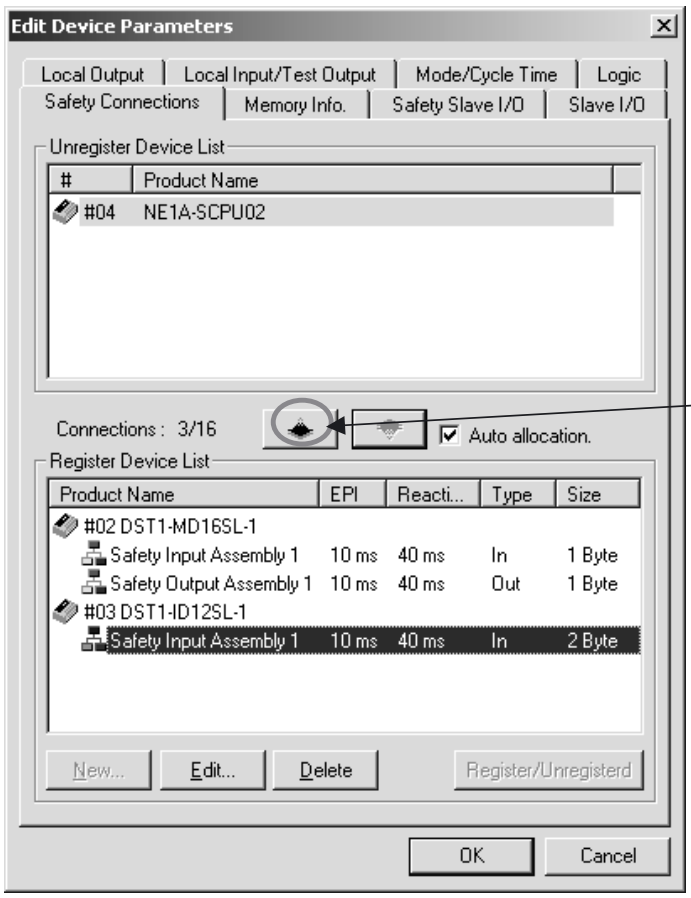
Nach dem Drücken der Schaltfläche zum Zurücknehmen der Registrierung wird die folgende Meldung angezeigt.



Klicken Sie auf **Yes**.

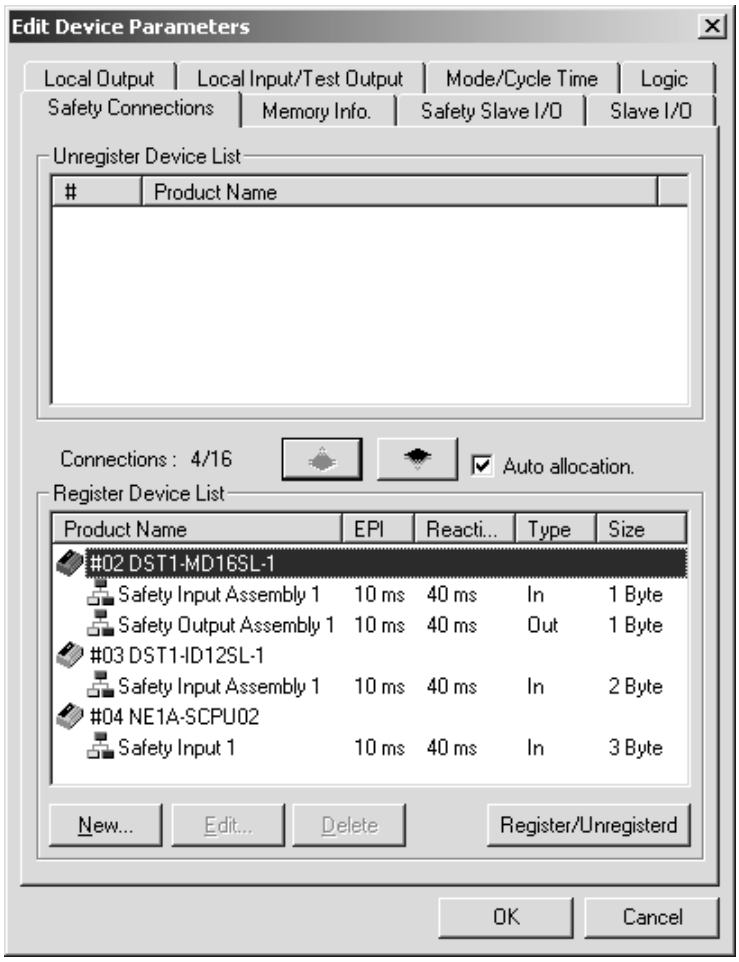
Nach der Rücknahme der Slave-Registrierung wird das folgende Fenster angezeigt.

Klicken Sie auf die Registrierungsschaltfläche, um den Slave erneut zu registrieren.



Wählen Sie den Slave aus, und klicken Sie auf diese Schaltfläche, um den Slave wieder zu registrieren.

Nach der Registrierung des Slaves wird das folgende Fenster angezeigt.

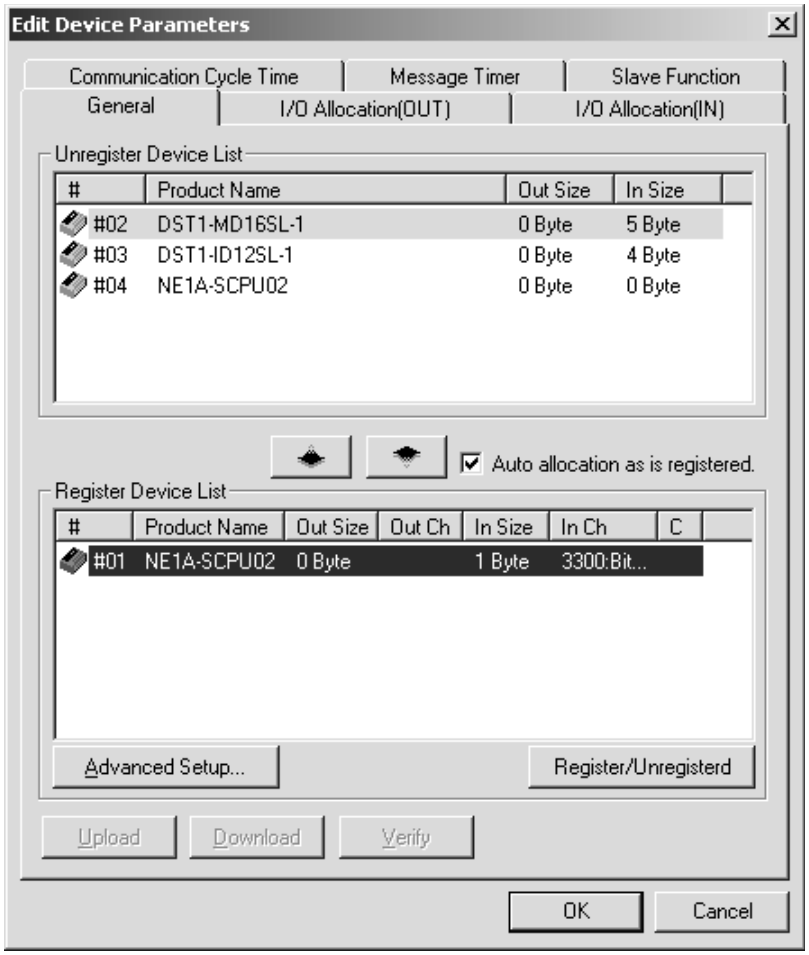


Klicken Sie auf **OK**. Damit ist der Vorgang abgeschlossen.

5. Neuregistrierung von Standard-Slaves für Standard-Master

Wenn das Gerät, dessen Konfigurationsdaten konvertiert werden, als Standard-Slave eingerichtet ist und der Produktcode des Geräts im Standard-Master ausgewählt wird, müssen die Einstellungen im Standard-Master geändert werden.

Wählen Sie das Gerät aus der Geräteliste der Registerkarte „General“ (Allgemein) im Fenster „Edit Device Parameters“ (Geräteparameter bearbeiten) für den Standard-Master aus.



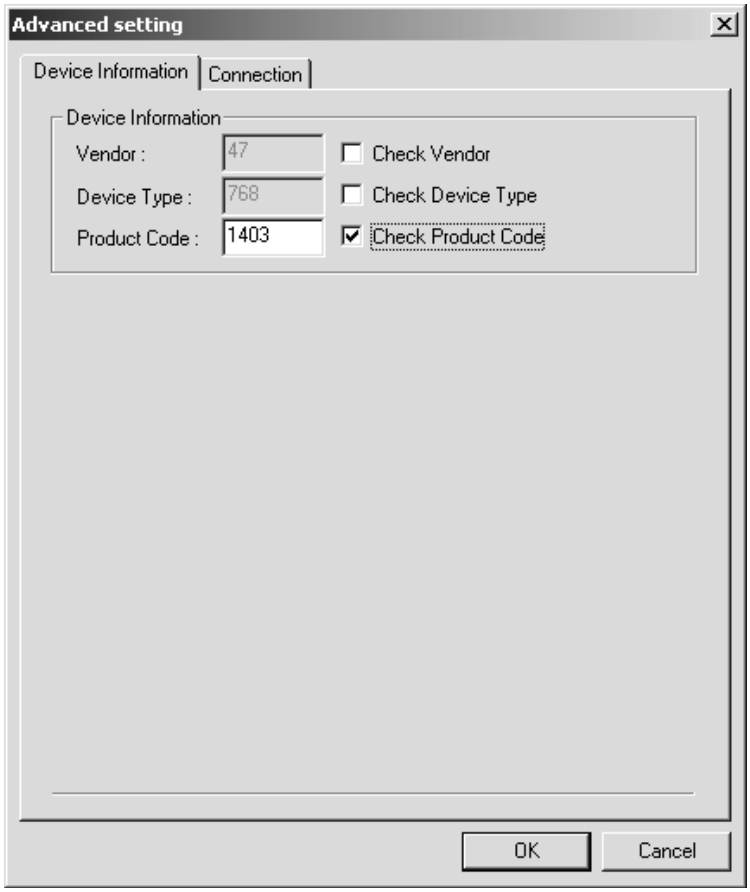
Klicken Sie dann auf **Advanced Setup**.

Wenn die Option „Check Product Code“ (Produktcode prüfen) auf der Registerkarte „Device Information“ (Geräteinformationen) im Fenster „Advanced Setting“ (Erweiterte Einstellung) aktiviert ist, ändern Sie den Produktcode entsprechend des zu verwendenden Geräts. Die Produktcodes lauten wie folgt:

NE1A-SCPU01: 1403

NE1A-SCPU01-V1: 1404

NE1A-SCPU02: 1405



Klicken Sie auf **OK**, nachdem Sie die Einstellung vorgenommen haben. Damit ist der Vorgang abgeschlossen.

ABSCHNITT 1
Überblick: Sicherheitsnetzwerk-Controller NE1A

1-1 Sicherheitsnetzwerk-Controller NE1A 2
1-1-1 Einführung: Sicherheitsnetzwerk-Controller NE1A. 2
1-1-2 Funktionsmerkmale des Sicherheitsnetzwerk-Controllers NE1A 3
1-1-3 Funktionsübersicht 5
1-1-4 E/A-Kapazitätsvergleich zwischen NE1A-SCPU01(-V1) und NE1A-SCPU02. 6
1-1-5 Verbesserte Funktionen der überarbeiteten Version 1.0 7
1-2 Systemkonfiguration 8
1-2-1 DeviceNet Safety Systemübersicht. 8
1-2-2 Beispiele für mögliche Systemkonfigurationen 9
1-3 Vorgehensweise bei der Einrichtung des Systems 16

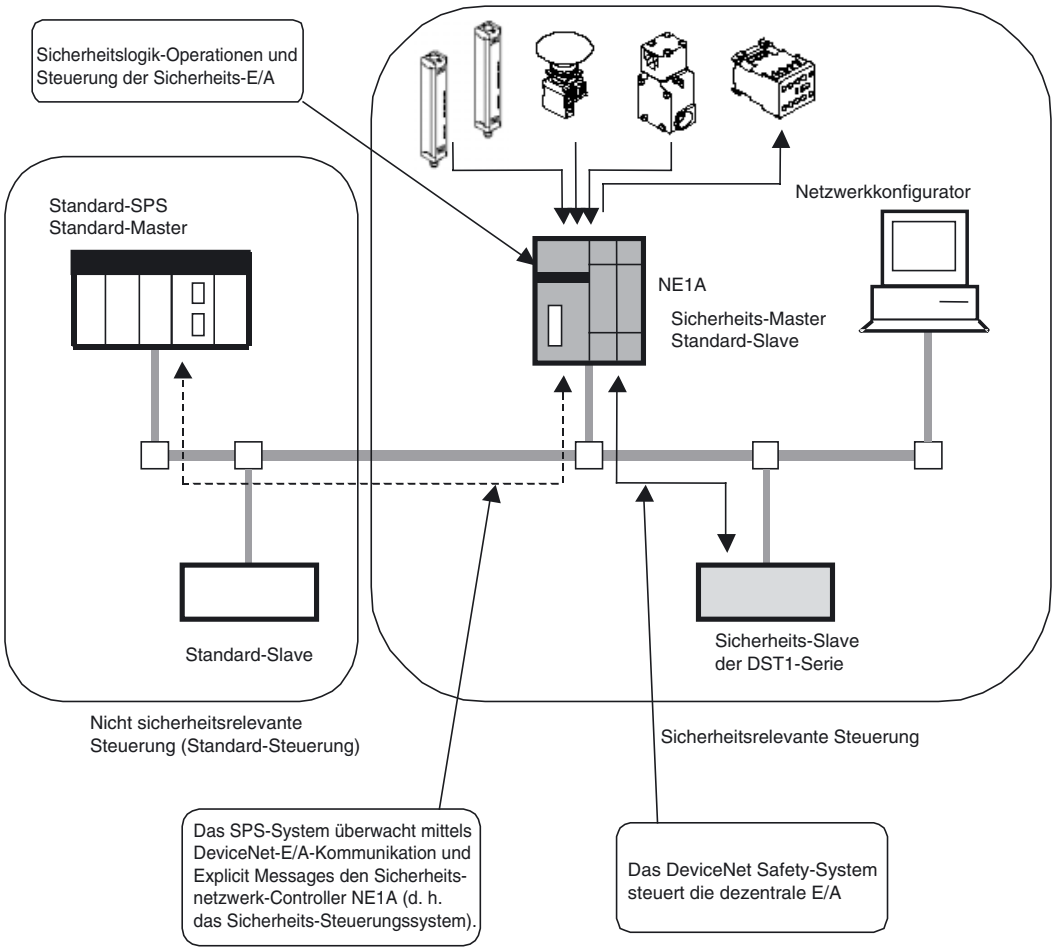
1-1 Sicherheitsnetzwerk-Controller NE1A

1-1-1 Einführung: Sicherheitsnetzwerk-Controller NE1A

Der Sicherheitsnetzwerk-Controller NE1A stellt verschiedene Funktionen wie Sicherheitslogik-Operationen, Sicherheits-E/A-Steuerung und ein DeviceNet Safety-Protokoll bereit. Der Sicherheitsnetzwerk-Controller NE1A ermöglicht den Aufbau einer Sicherheitssteuerung/eines Netzwerksystems, die/das den Anforderungen für die unter IEC 61508 (Funktionale Sicherheit von elektrischen/elektronischen/programmierbaren Sicherheitssystemen) definierte Sicherheitsintegritätsstufe 3 und den Anforderungen der Steuerungskategorie 4 gemäß EN 954-1 entspricht.

In dem unten dargestellten Beispielsystem wird das mit einem Sicherheitsnetzwerk-Controller NE1A implementierte Sicherheits-Steuerungssystem und das mit der Standard-SPS implementierte Überwachungssystem in demselben Netzwerk realisiert.

- Als Sicherheitslogik-Controller führt der Sicherheitsnetzwerk-Controller NE1A Sicherheitslogik-Operationen aus und steuert die lokale E/A.
- Als Sicherheits-Master steuert der Sicherheitsnetzwerk-Controller NE1A die dezentrale E/A von Sicherheits-Slaves.
- Als Standard-DeviceNet-Slave kommuniziert der Sicherheitsnetzwerk-Controller NE1A mit dem Standard-DeviceNet-Master.



1-1-2 Funktionsmerkmale des Sicherheitsnetzwerk-Controllers NE1A

Sicherheitslogik-Operationen

Ergänzend zu den grundlegenden Logik-Funktionen wie AND und OR werden Funktionsblöcke wie die Überwachung von NOT-AUS-Tastern und Sicherheitstüren unterstützt, die die Realisierung der verschiedensten Sicherheitsanwendungen ermöglichen.

Lokale Sicherheits-E/A

- NE1A-SCPU01(-V1) unterstützt insgesamt 24 lokale Sicherheits-E/A-Punkte: 16 Eingänge und 8 Ausgänge.
- NE1A-SCPU02 unterstützt insgesamt 48 lokale Sicherheits-E/A-Punkte: 40 Eingänge und 8 Ausgänge.
- Fehler in der externen Verdrahtung können aufgedeckt werden.
- Paare zusammengehöriger lokaler Eingänge können im Zweikanal-Modus betrieben werden.
  In diesem Modus kann der Sicherheitsnetzwerk-Controller NE1A die Eingangsdaten-Muster und die Zeitabweichungen zwischen den Eingangssignalen analysieren.
- Paare zusammengehöriger lokaler Ausgänge können im Zweikanal-Modus betrieben werden. In diesem Modus kann der Sicherheitsnetzwerk-Controller NE1A die Ausgangsdaten-Muster analysieren.

DeviceNet Safety-Kommunikation

- Als Sicherheits-Master können Sicherheitsnetzwerk-Controller vor Version 1.0 Sicherheits-Kommunikation über bis zu 16 Verbindungen mit bis zu 16 Bytes je Verbindung durchführen.
- Der Sicherheitsnetzwerk-Controller NE1A der Version 1.0 kann Sicherheits-Kommunikation über bis zu 32 Verbindungen mit bis zu 16 Bytes je Verbindung durchführen.
- Als Sicherheits-Slave kann der Sicherheitsnetzwerk-Controller NE1A Sicherheits-Kommunikation über bis zu 16 Verbindungen mit bis zu 16 Bytes je Verbindung durchführen.

DeviceNet-Standard-Kommunikation

Als Standard-Slave kann der Sicherheitsnetzwerk-Controller NE1A Standard-Kommunikation mit einem Standard-Master über bis zu zwei Verbindungen mit bis zu 16 Bytes je Verbindung durchführen.

Standalone-Controller-Modus

Der Sicherheitsnetzwerk-Controller NE1A kann nach Deaktivierung der DeviceNet-Kommunikation auch als Standalone-Controller eingesetzt werden.

Konfiguration mittels eines grafischen Tools

- Die Netzwerkkonfiguration und die Logik-Programmierung erfolgen mithilfe eines grafischen Tools. Dieses ermöglicht eine problemlose Konfiguration und Programmierung.
- Ein Logikeditor kann vom Netzwerkkonfigurator aus aktiviert werden.
- Konfigurationsdaten können herauf- und heruntergeladen werden, und Geräte können online über DeviceNet, USB oder die periphere Schnittstelle einer OMRON-SPS überwacht werden.

Systemstart und Unterstützung für das Wiederaufsetzen nach Fehlern (Error Recovery)

- Der Netzwerkkonfigurator und die Anzeigen an der Front des Sicherheitsnetzwerk-Controllers NE1A vereinfachen die Fehlersuche.
- Die internen Statusinformationen des Sicherheitsnetzwerk-Controllers NE1A können von einer Standard-SPS aus überwacht werden, indem diese Informationen im Standard-Master zugeteilt werden. Auf die gleiche Weise ist eine Überwachung durch eine Sicherheits-SPS möglich, indem diese Informationen im Sicherheits-Master zugeteilt werden.

Zugangsbeschränkung durch Passwort

- Die Konfigurationsdaten des Sicherheitsnetzwerk-Controllers NE1A sind durch ein Passwort geschützt.
- Der Netzwerkkonfigurator schützt den Zugriff auf die einzelnen Projektdateien durch ein Passwort.

1-1-3 Funktionsübersicht

Funktion	Übersicht	Details
Logik-Operationen		
Logik-Operationen	Grundlegende Logik-Funktionen wie AND und OR sowie Funktionsblöcke NOT-AUS (ESTOP) und Sicherheitstürüberwachung (SGATE). Bei der Programmierung von Controllern vor Version 1.0 können maximal 128 Logik-Funktionen und Funktionsblöcke verwendet werden. Bei der Programmierung von Controllern ab Version 1 können maximal 254 Logik-Funktionen und Funktionsblöcke verwendet werden.	Kapitel 6
Sicherheits-E/A		
E/A-Kommentare	Jeder E/A-Klemme kann ein maximal 32 ASCII-Zeichen langer Namen zugeordnet werden.	5-1-1
Überwachung der E/A-Spannungsversorgung	Der Sicherheitsnetzwerk-Controller NE1A kann feststellen, ob die E/A-Spannungsversorgung im zulässigen Spannungsbereich liegt.	5-1-2
Sicherheitseingänge	Der Sicherheitsnetzwerk-Controller NE1A-SCPU01(-V1) unterstützt 16 Sicherheitseingänge. Der Sicherheitsnetzwerk-Controller NE1A-SCPU02 unterstützt 40 Sicherheitseingänge.	5-2
Eingangsschaltkreis-diagnose	Mittels Testimpulsen kann eine Diagnose der internen Schaltkreise des Sicherheitsnetzwerk-Controllers NE1A, der externen Geräte und der externen Verdrahtung durchgeführt werden.	
Eingangsverzögerungen (Einschalt- und Ausschaltverzögerungen)	Für die Eingänge des Sicherheitsnetzwerk-Controllers NE1A können Verzögerungszeiten zwischen 0 und 126 ms (jeweils als Vielfache der Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A) eingestellt werden. Diese Eingangsverzögerungen erleichtern die Unterdrückung von Kontaktprellen und Störeinflüssen.	
Zweikanal-Modus	Die Zeitabweichung zwischen der Änderung des Zustands eines von zwei im Zweikanalmodus betriebenen Eingängen bis zur Änderung des Zustands des anderen Eingangs kann ermittelt und ausgewertet werden.	
Testausgänge	Der Sicherheitsnetzwerk-Controller NE1A-SCPU01(-V1) besitzt vier voneinander unabhängige Testausgänge. Der Sicherheitsnetzwerk-Controller NE1A-SCPU02 besitzt acht voneinander unabhängige Testausgänge. Diese werden normalerweise in Kombination mit Sicherheitseingängen verwendet, können jedoch auch als Signalausgänge eingesetzt werden.	5-3
Stromüberwachung für Muting-Lampe (nur Klemme T3, T7)	Der Sicherheitsnetzwerk-Controller NE1A-SCPU01(-V1) kann eine Unterbrechung an Klemme T3 erkennen. Der Sicherheitsnetzwerk-Controller NE1A-SCPU02 kann eine Unterbrechung an den Klemmen T3 und T7 erkennen.	
Überstrom-Erkennung/ Schutz	Zum Schutz des Schaltkreises wird beim Erkennen eines Überstroms der entsprechende Ausgang blockiert.	
Sicherheitsausgänge	NE1A-SCPU01(-V1) und NE1A-SCPU02 besitzen je acht Sicherheitsausgänge.	5-4
Ausgangsschaltkreis-diagnose	Mittels Testimpulsen kann eine Diagnose der internen Schaltkreise des Sicherheitsnetzwerk-Controllers NE1A, der externen Geräte und der externen Verdrahtung durchgeführt werden.	
Überstrom-Erkennung/ Schutz	Zum Schutz des Schaltkreises wird beim Erkennen eines Überstroms der entsprechende Ausgang blockiert.	
Zweikanal-Modus	Beim Auftreten eines Fehlers in einem von zwei im Zweikanalmodus betriebenen lokalen Ausgängen können beide Ausgänge in den Sicherheitszustand versetzt werden, ohne dass dies entsprechende Vorkehrungen im Anwenderprogramm erfordert.	
DeviceNet-Kommunikation		
Sicherheits-Master	Für jede Verbindung im DeviceNet Safety-Netzwerk wird eine von der Master-Slave-Kommunikation im DeviceNet-Standard-Netzwerk unabhängige Master-Slave-Beziehung eingerichtet. Dies ermöglicht dem Sicherheitsnetzwerk-Controller NE1A die Steuerung der Verbindungen als Sicherheits-Master.	4-4

Funktion	Übersicht	Details
Sicherheits-Slave	Der Sicherheitsnetzwerk-Controller NE1A kann auch als Sicherheits-Slave fungieren, wobei sowohl die internen Statusinformationen als auch ein spezifizierter E/A-Bereich im Sicherheits-Master zugeteilt werden können.	4-5
Standard-Slave	Der Sicherheitsnetzwerk-Controller NE1A kann auch als Standard-Slave fungieren, wobei sowohl die internen Statusinformationen als auch ein spezifizierter E/A-Bereich im Standard-Master zugeteilt werden können.	4-6
Explicit Messages	Die Statusinformationen des Sicherheitsnetzwerk-Controllers NE1A können mithilfe von Explicit Messages ausgelesen werden. Außerdem kann vom Anwenderprogramm aus eine mithilfe des Netzwerkkonfigurators festgelegte Explicit Message versendet werden.	4-7
Automatische Erkennung der Baudrate	Die Baudrate des Sicherheitsnetzwerk-Controllers NE1A kann automatisch auf die Baudrate des Netzwerk-Masters eingestellt werden.	4-1-1
Standalone-Controller-Modus		
Standalone-Controller-Modus	Der Sicherheitsnetzwerk-Controller NE1A kann durch Deaktivierung der DeviceNet-Kommunikation auch als Standalone-Controller eingesetzt werden.	4-1-2
Systemstart und Unterstützung für das Wiederaufsetzen nach Fehlern		
Fehlerprotokoll	Im Fehlerprotokoll des Sicherheitsnetzwerk-Controllers NE1A werden die vom Sicherheitsnetzwerk-Controller NE1A erkannten Fehler einschließlich der Gesamtbetriebszeit zum Zeitpunkt des Fehlers aufgezeichnet.	10-4
Online-Überwachung	Die internen Statusinformation des Sicherheitsnetzwerk-Controllers NE1A sowie die E/A-Daten können mithilfe des Netzwerkkonfigurators online überwacht werden.	Systemkonfigurations-Handbuch, Abschnitt 7
Weitere Funktionen		
Konfigurationsschutz	Die im Sicherheitsnetzwerk-Controller NE1A gespeicherten heruntergeladenen und verifizierten Konfigurationsdaten können gesperrt werden, um die Daten vor unautorisierter Änderung zu schützen.	7-1
Reset	Der Sicherheitsnetzwerk-Controller NE1A kann mithilfe des Netzwerkkonfigurators zurückgesetzt werden.	7-2
Passwort	Durch Setzen eines Passworts kann ein unbeabsichtigter oder unautorisierter Zugriff auf den Sicherheitsnetzwerk-Controller NE1A verhindert werden.	7-3

1-1-4 E/A-Kapazitätsvergleich zwischen NE1A-SCPU01(-V1) und NE1A-SCPU02

Parameter	NE1A-SCPU01	NE1A-SCPU02	Verweis
Anzahl der E/A-Punkte			
Sicherheitseingänge	16	40	2-1
Testausgänge	4	8	2-1
Sicherheitsausgänge	8	8	2-1

1-1-5 Verbesserte Funktionen der überarbeiteten Version 1.0

Die nachstehende Tabelle beschreibt die an Version 1.0 vorgenommenen Änderungen.

Funktion	Zusammenfassung	Verweis
Logik-Operationen		
Logik-Operationen	Bei der Programmierung können bis zu 254 Logik-Funktionen und Funktionsblöcke verwendet werden.	Kapitel 6
Funktionsblöcke	Folgende Funktionsblöcke können zusätzlich verwendet werden: Logik-Funktionen • RS Flip-flop • Komparator Funktionsblöcke • Muting • Zustimmschalter • Impulsgeber • Zähler • Multi Connector	Kapitel 6
Angabe der Rücksetzbedingungen für die Funktionsblöcke „Reset“ und „Restart“	Folgende Rücksetzbedingungen stehen zur Auswahl: • Low - High - Low EIN Impuls (Rücksetzbedingung der Vorläuferversionen) • Low - High steigende Flanke	Kapitel 6
E/A-Steuerungsfunktionen		
Nutzbare Daten für E/A-Tags	Folgende E/A-Tags können zusätzlich verwendet werden: • Zustand der lokalen E/A • Allgemeiner Gerätezustand	6-1-2
Schalthäufigkeitszähler	Die Anzahl der EIN- und AUS-Schaltvorgänge an einem Ein- oder Ausgang kann gezählt und intern gespeichert werden.	5-1-3
Gesamteinschaltdauer-Überwachung	Die Einschaltzeit eines Ein- oder Ausgangs kann gemessen und intern gespeichert werden.	5-1-4
DeviceNet-Kommunikationsfunktionen		
Sicherheits-Master-Funktion	Es können bis zu 32 Verbindungen genutzt werden.	4-4
Angabe des Sicherheits-E/A-Kommunikationsstatus nach Auftreten eines Kommunikationsfehlers	Der Benutzer kann einen der folgenden Zustände für die Sicherheits-E/A-Kommunikation nach dem Auftreten von Kommunikationsfehlern festlegen. • Automatische Rücksetzung (Funktion der Vorläuferversionen) • Nur die Verbindung anhalten, an der der Fehler aufgetreten ist. • Alle Verbindungen anhalten	4-4
Neustart von E/A-Kommunikationen, die aufgrund von Kommunikationsfehlern unterbrochen wurden	Wenn die Sicherheits-E/A-Kommunikation aufgrund eines Kommunikationsfehlers unterbrochen wurde, kann sie über den Netzwerkkonfigurator oder das Logik-Programm neu gestartet werden.	4-4
Dezentrale E/A-Zuordnung	Wenn der Controller als Sicherheits-Slave oder Standard-Slave mit Eingängen arbeitet, können folgende Daten an die Sendedaten angehängt werden. • Lokale Eingangsüberwachung • Lokale Ausgangsüberwachung	4-3
Systemstart und Unterstützung für das Wiederaufsetzen nach Fehlern		
Speichern des Fehlerprotokolls	Das Protokoll geringfügiger Fehler wird im nichtflüchtigen Speicher gespeichert.	10-3
Zusatzpositionen für Fehlerprotokoll	Fehler, die in Funktionsblöcken auftreten, werden im Fehlerprotokoll aufgezeichnet.	10-4

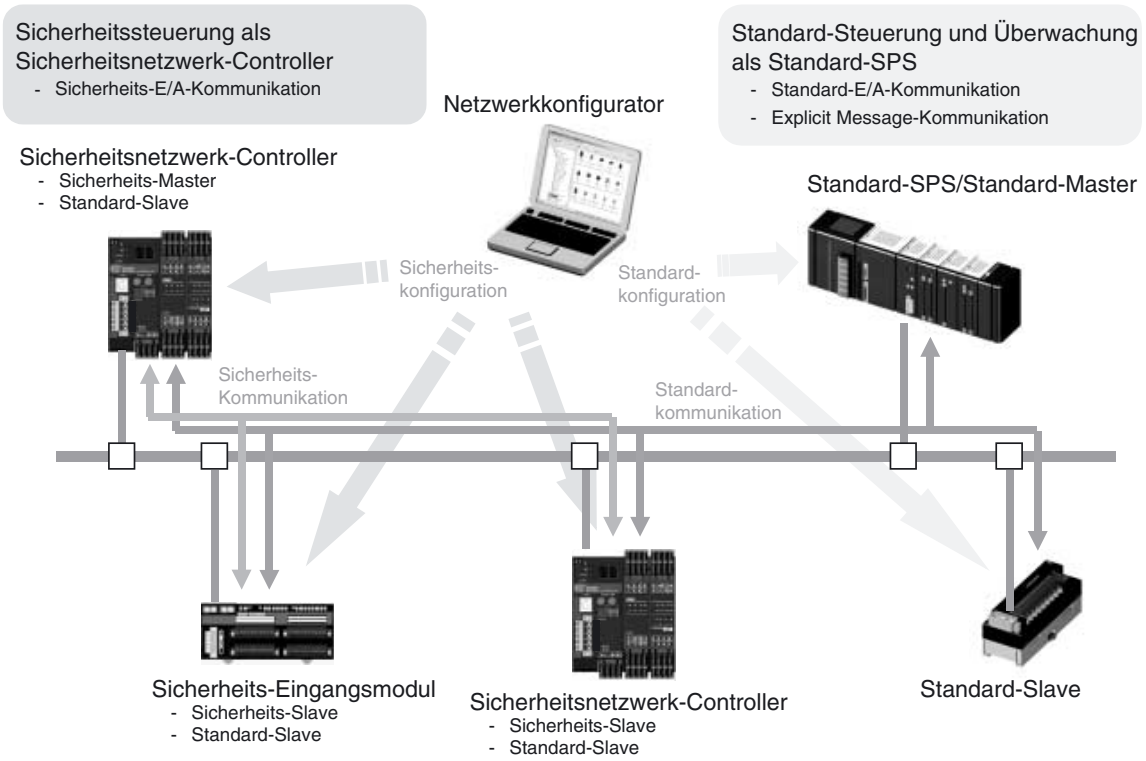
1-2 Systemkonfiguration

1-2-1 DeviceNet Safety Systemübersicht

DeviceNet ist ein der Open Field-Spezifikation entsprechendes Multi-Vendor-/ Multi-Bit-Netzwerk, das die Steuerungen in der Maschine miteinander verknüpft. Das DeviceNet Safety-Netzwerk erweitert das konventionelle Standard-DeviceNet-Kommunikationsprotokoll um Sicherheitsfunktionen. Das DeviceNet Safety-Konzept wurde durch eine unabhängige Organisation (TÜV Rheinland) geprüft und anerkannt.

Ebenso wie bei DeviceNet können auch an DeviceNet Safety-Netzwerke DeviceNet Safety-Geräte von Drittanbietern angeschlossen werden. Darüber hinaus können DeviceNet- und DeviceNet Safety-Geräte kombiniert und an ein und dasselbe Netzwerk angeschlossen werden.

Die Kombination von DeviceNet Safety-Produkten ermöglicht den Aufbau einer Sicherheitssteuerung/eines Netzwerksystems, die/das den Anforderungen für die unter IEC 61508 (Funktionale Sicherheit von elektrischen/elektronischen/ programmierbaren Sicherheitssystemen) definierte Sicherheitsintegritätsstufe 3 und den Anforderungen der Sicherheitskategorie 4 gemäß EN 954-1 entspricht.



1-2-2 Beispiele für mögliche Systemkonfigurationen

Die folgenden Beispiele illustrieren die Realisierung von Sicherheitssteuerungssystemen mithilfe des Sicherheitsnetzwerk-Controllers NE1A.

- Sicherheitssteuerungssystem mit einem Sicherheitsnetzwerk-Controller NE1A als Sicherheits-Master
- Kombiniertes System aus einem Sicherheitssteuerungssystem mit einem Sicherheitsnetzwerk-Controller NE1A als Sicherheits-Master und einer Standard-SPS als Überwachungssystem
- Kombiniertes System aus einem verteilten Sicherheitssteuerungssystem mit mehreren als Sicherheits-Master fungierenden Sicherheitsnetzwerk-Controllern NE1A und einem zentralisierten Überwachungssystem mit Standard-SPS
- Sicherheitsnetzwerk-Controller NE1A als Standalone-System
- Verbindung mit dem Netzwerkkonfigurator

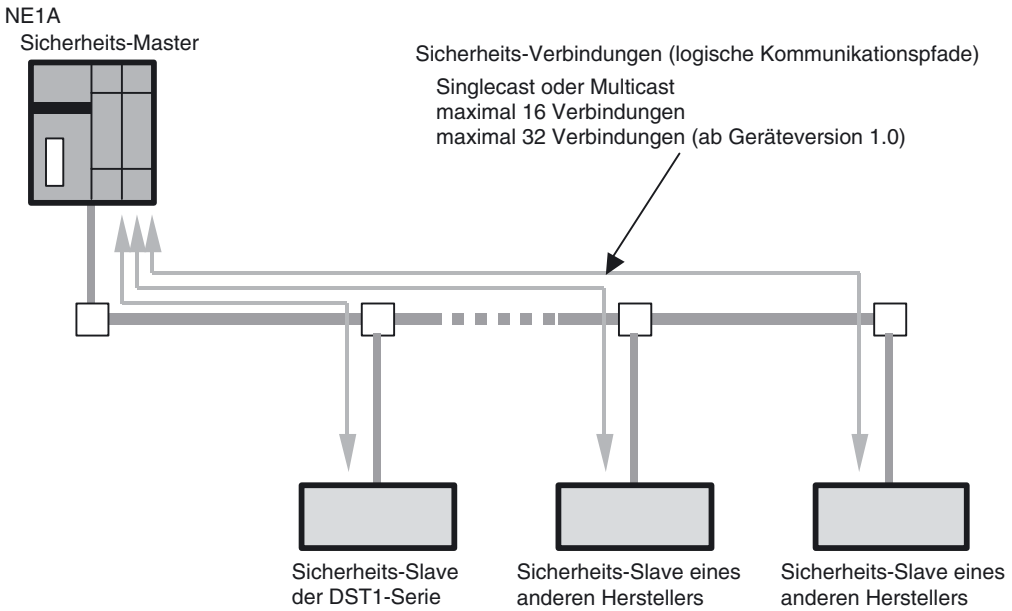
Sicherheitssteuerungssystem mit einem Sicherheitsnetzwerk-Controller NE1A als Sicherheits-Master

Dieses System nutzt den Sicherheitsnetzwerk-Controller NE1A als Sicherheits-Master, der die Sicherheits-Slaves in diesem dezentralen Sicherheits-E/A-System steuert und überwacht.

Als Sicherheits-Master können die Sicherheitsnetzwerk-Controller vor Version 1.0 Sicherheits-EA-Kommunikation über bis zu 16 Verbindungen (16 Slaves) mit bis zu 16 Bytes je Verbindung durchführen.

Sicherheitsnetzwerk-Controller ab Version 1.0 können als Sicherheits-Master Sicherheits-EA-Kommunikation über bis zu 32 Verbindungen (32 Slaves) mit bis zu 16 Bytes je Verbindung durchführen.

Der Sicherheitsnetzwerk-Controller NE1A unterstützt für Sicherheits-E/A-Verbindungen das Singlecast- und das Multicast-Protokoll (Broadcast).



Kombiniertes System aus einem Sicherheitssteuerungssystem und einem SPS-Überwachungssystem

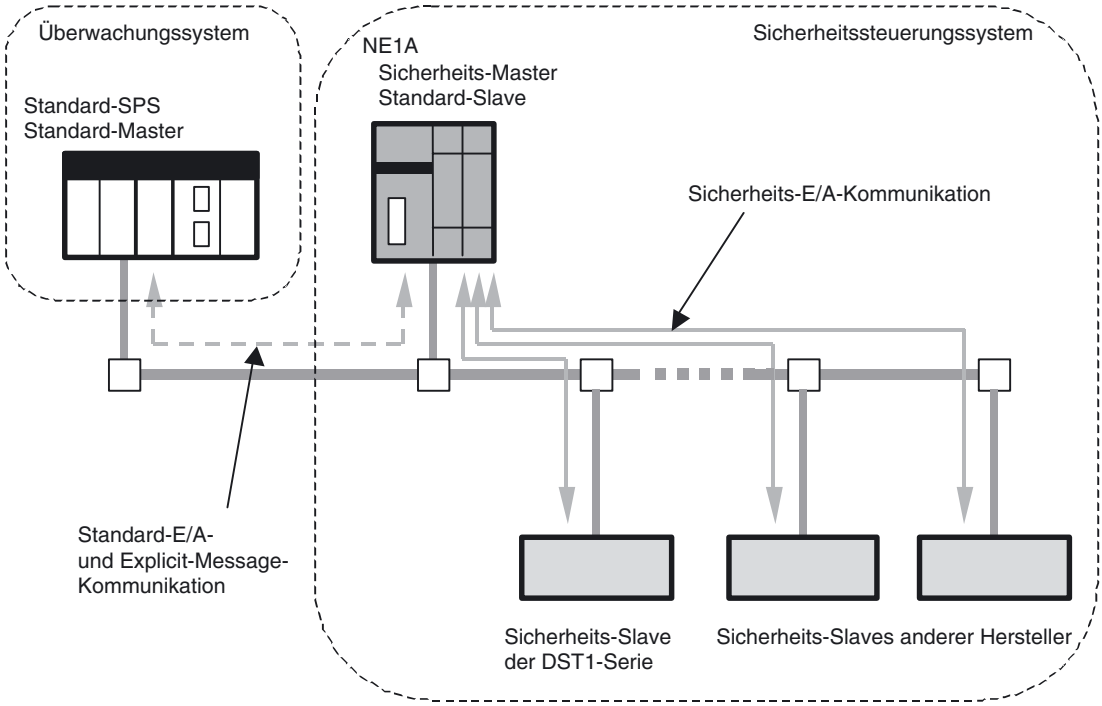
Dieses System nutzt den Sicherheitsnetzwerk-Controller NE1A als Sicherheits-Master, der die Sicherheits-Slaves in diesem dezentralen Sicherheits-E/A-System steuert und überwacht.

Für die Überwachungskomponente wird der Sicherheitsnetzwerk-Controller NE1A als Standard-Slave genutzt, der über Standard-E/A-Kommunikation mit dem Standard-Master kommuniziert. Der Sicherheitsnetzwerk-Controller NE1A fungiert gleichzeitig als Sicherheits-Master und als Standard-Slave.

Als Standard-Slave kann der Sicherheitsnetzwerk-Controller NE1A Standard-E/A-Kommunikation über bis zu zwei Verbindungen mit bis zu 16 Bytes je Verbindung durchführen. Für E/A-Verbindungen werden vier Protokolle (Poll, Bitstrobe, COS und Cyclic) unterstützt. Der Sicherheitsnetzwerk-Controller NE1A kann nicht als Standard-Master fungieren.

Das Sicherheitssteuerungssystem kann durch eine Standard-SPS überwacht werden. Dazu können die Statusinformationen des Sicherheitsnetzwerk-Controllers NE1A (allgemeiner Status, Fehlerstatus usw.) in der Standard-SPS zugeteilt oder die Ergebnisse von Logikoperationen über Standard-E/A-Kommunikation an die Standard-SPS übermittelt werden.

Sicherheits- und Überwachungssystem können kombiniert und mit Standard- und Sicherheitsgeräten in ein und demselben Netzwerk realisiert werden.



WICHTIG Insgesamt können bis zu 64 Standard- und Sicherheitsknoten an das Netzwerk angeschlossen werden.
Bei den durch Standard-E/A- und Explicit Message-Kommunikation übertragenen Datenattributen handelt es sich um Nicht-Sicherheits-Daten. Bei der Generierung dieser Daten werden die erforderlichen Maßnahmen für Sicherheitsdaten nicht ergriffen. Diese Daten dürfen daher nicht für die Konfiguration des Sicherheitssteuerungssystems eingesetzt werden.

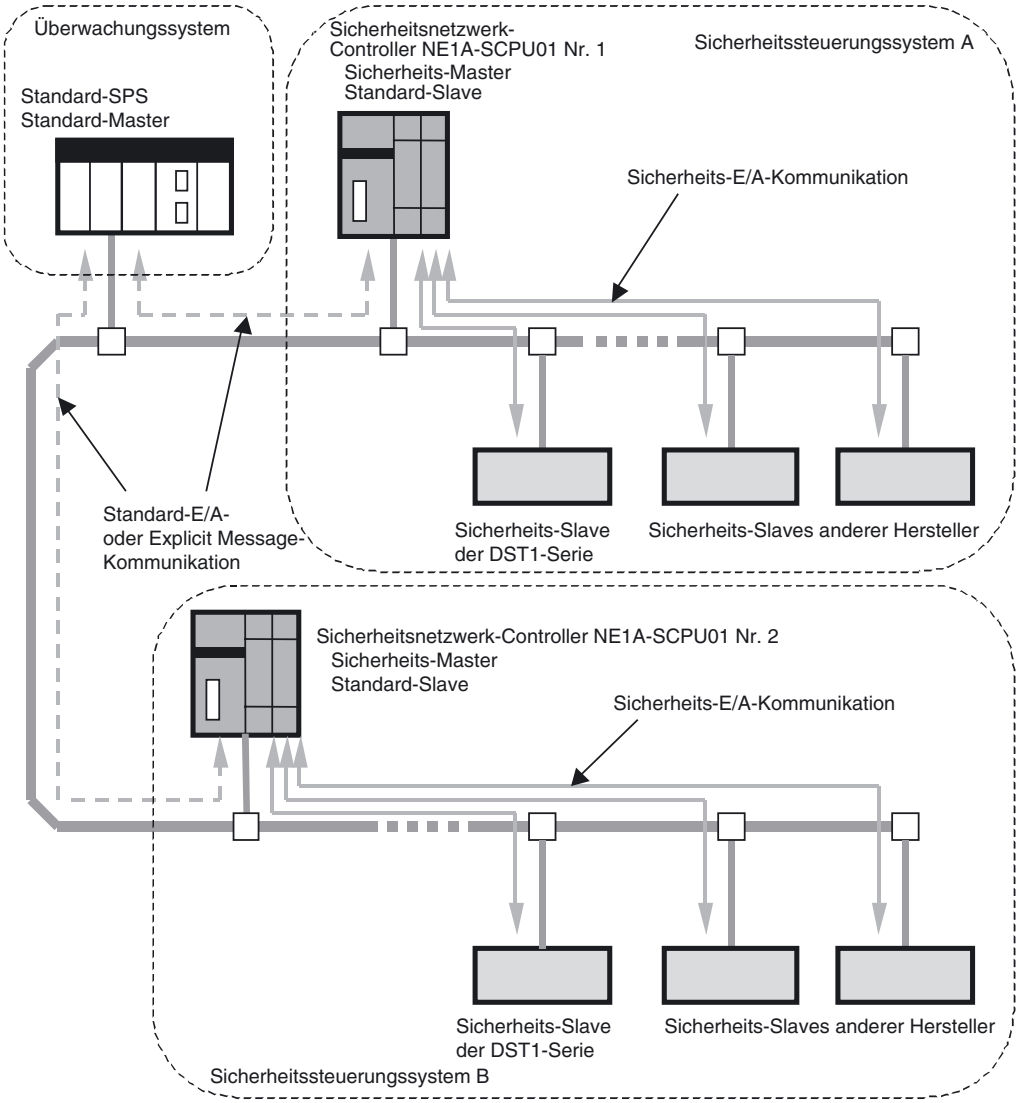
Kombiniertes System aus einem verteilten Sicherheitssteuerungssystem mit mehreren als Sicherheits-Master fungierenden Sicherheitsnetzwerk-Controllern NE1A und einem zentralisierten Überwachungssystem

Dieses System nutzt mehrere Sicherheitsnetzwerk-Controller NE1A als Sicherheits-Master, die die Sicherheits-Slaves in diesem dezentralen Sicherheits-E/A-System steuern und überwachen.

Dabei fungieren die Sicherheitsnetzwerk-Controller NE1A gleichzeitig als Standard-Slaves, die über Standard-E/A-Kommunikation mit dem Standard-Master kommunizieren.

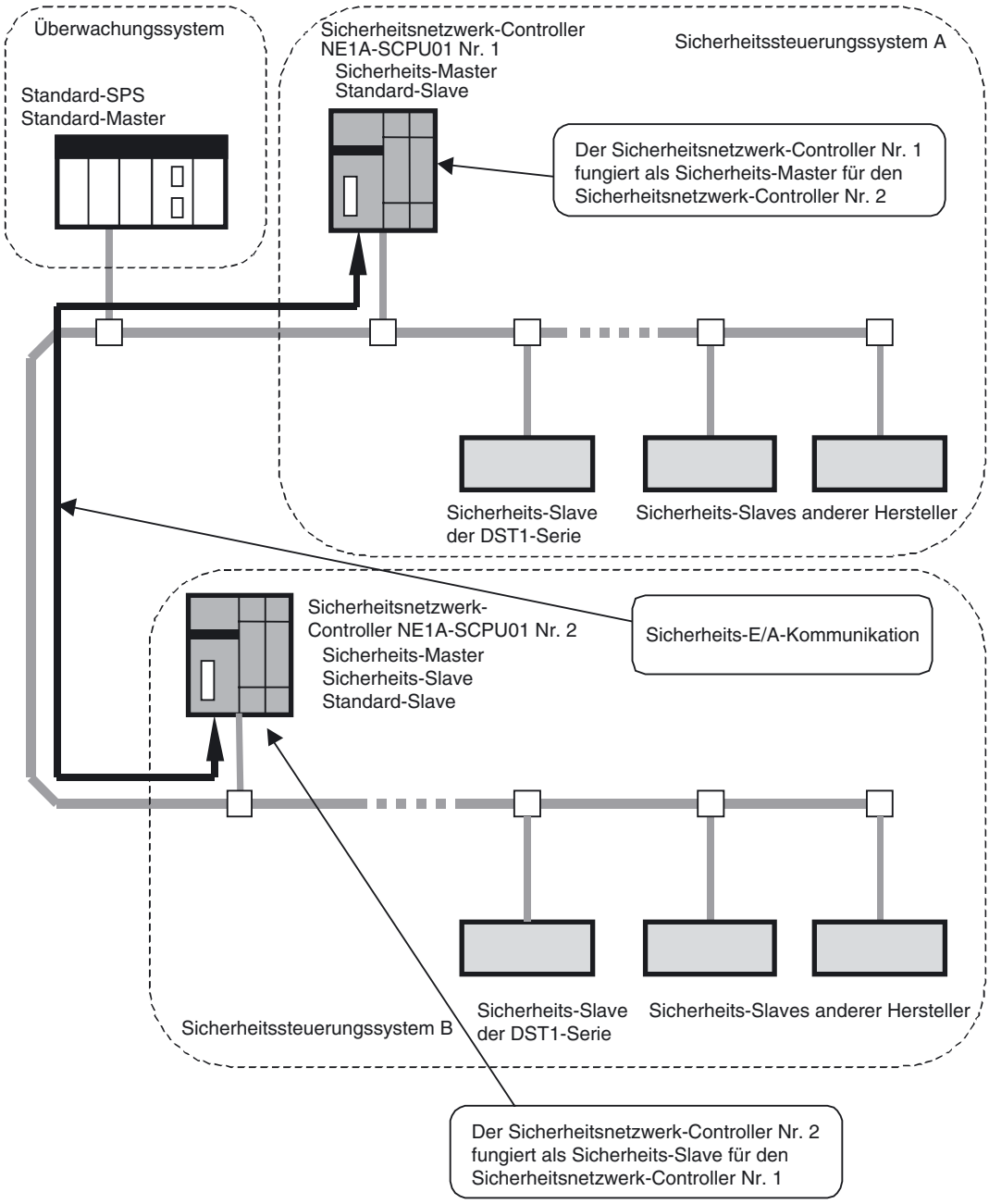
Das Sicherheitssteuerungssystem kann durch eine Standard-SPS überwacht werden. Dazu können die Statusinformationen des Sicherheitsnetzwerk-Controllers NE1A (allgemeiner Status, Fehlerstatus usw.) oder die Ergebnisse von Logikoperationen in der Standard-SPS zugeteilt werden.

Innerhalb eines DeviceNet Safety-Sicherheitsnetzwerks können mehrere Sicherheits-Master eingesetzt werden. Auf diese Weise können die verteilten Blöcke der Sicherheitssteuerung zentral im selben Netzwerk überwacht werden.



Außerdem kann wie im folgenden Diagramm illustriert eine Sicherheits-E/A-Kommunikation zwischen den einzelnen Sicherheitsnetzwerk-Controllern NE1A stattfinden. In diesem Diagramm fungiert der Sicherheitsnetzwerk-Controller Nr. 1 als Slave des Sicherheitsnetzwerk-Controllers Nr. 2.

Der Sicherheitsnetzwerk-Controller NE1A fungiert gleichzeitig als Sicherheits-Master, als Sicherheits-Slave und als Standard-Slave. Als Sicherheits-Slave kann der Sicherheitsnetzwerk-Controller NE1A Sicherheits-E/A-Kommunikation über bis zu vier Verbindungen mit bis zu 16 Bytes je Verbindung durchführen.

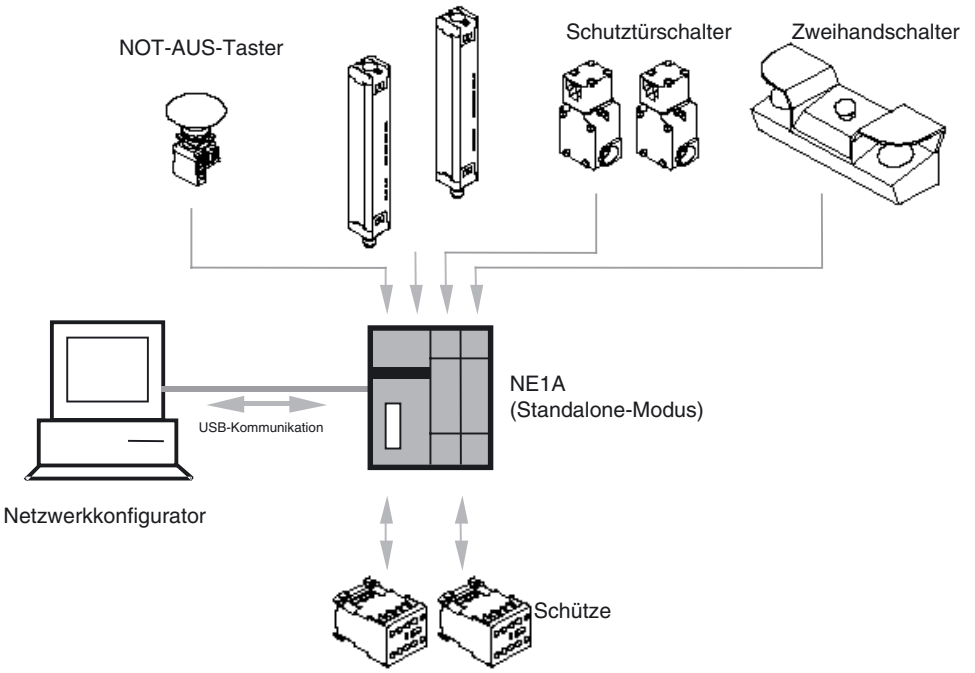


WICHTIG Bei den durch DeviceNet Standard-E/A- und Explicit Message-Kommunikation übertragenen Datenattributen handelt es sich um Nicht-Sicherheits-Daten. Bei der Generierung dieser Daten werden die erforderlichen Maßnahmen für Sicherheitsdaten nicht ergriffen. Diese Daten dürfen daher nicht für die Konfiguration des Sicherheitssteuerungssystems eingesetzt werden.

Sicherheitsnetzwerk-Controller NE1A als Standalone-System

Erfordert die Anwendung nur die Steuerung einiger weniger E/A-Punkte, kann der Sicherheitsnetzwerk-Controller NE1A auch als Standalone-Controller eingesetzt werden.

Dazu muss durch entsprechende Einstellungen im Netzwerkkonfigurator die DeviceNet-Kommunikation des Sicherheitsnetzwerk-Controllers NE1A deaktiviert werden.



WICHTIG Zur Deaktivierung der DeviceNet-Kommunikation des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 muss dieser über eine USB-Verbindung mit dem Netzwerkkonfigurator-PC verbunden sein. Die Deaktivierung der DeviceNet-Kommunikation kann logischerweise nicht über die DeviceNet-Schnittstelle erfolgen.

Verbindung mit dem Netzwerkkonfigurator

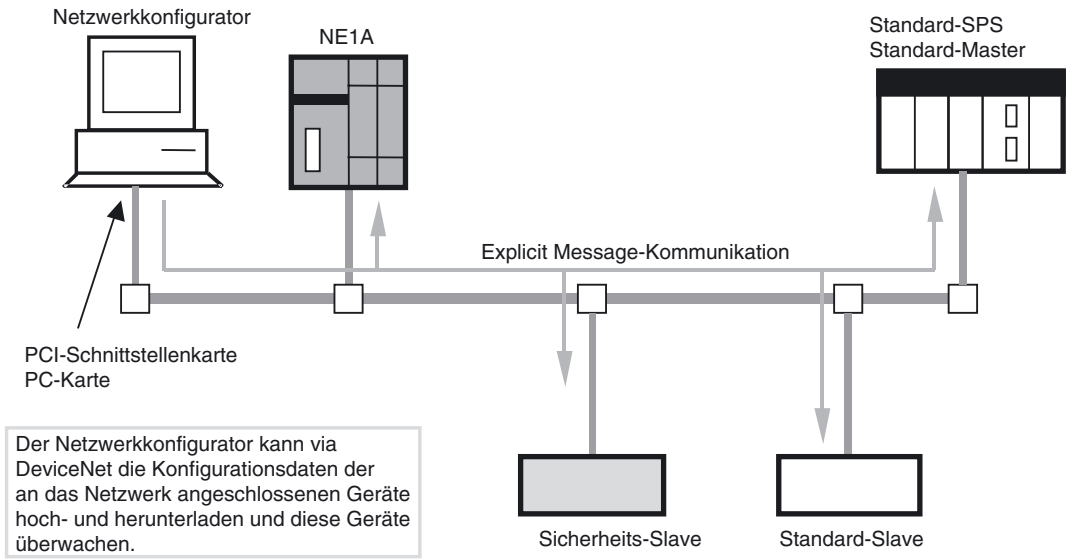
Die Konfiguration und Programmierung des Sicherheitsnetzwerk-Controllers NE1A erfolgt mithilfe des Netzwerkkonfigurators. Dieser ermöglicht auch das Hochladen der Konfigurationsdaten, die Online-Überwachung des Ausführungszustands von Programmen, das Abrufen des Fehlerprotokolls usw.

Der Netzwerkkonfigurator kann auf dreierlei Weise verbunden werden:

- Direkte Verbindung mit dem DeviceNet-Netzwerk
- USB-Verbindung mit dem Sicherheitsnetzwerk-Controller NE1A
- Serielle Verbindung mit einer OMRON SPS

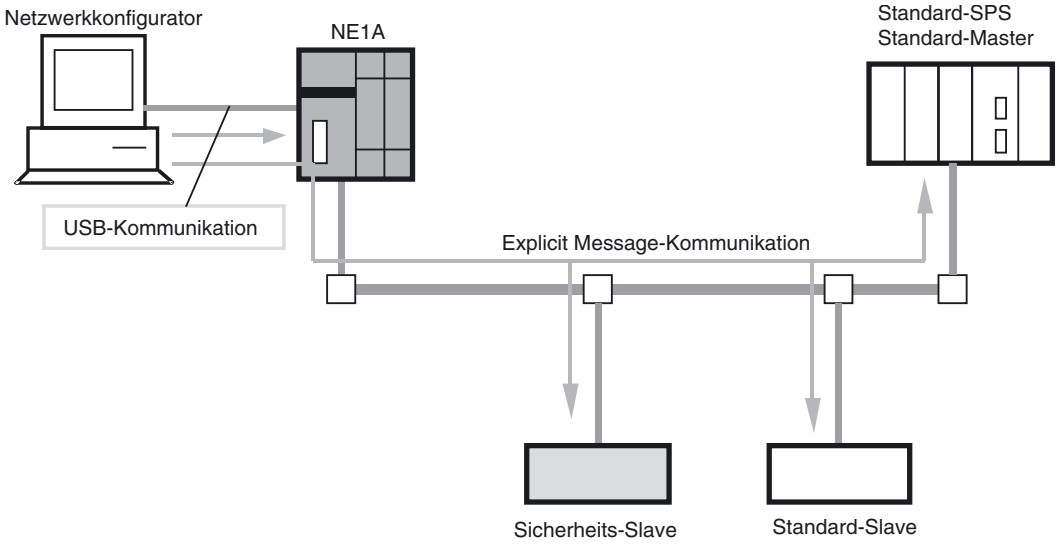
Direkte Verbindung mit dem DeviceNet-Netzwerk

Bei Verwendung einer DeviceNet-Schnittstellenkarte im Netzwerkkonfigurator-PC kann dieser direkt an das DeviceNet-Netzwerk angeschlossen werden. Auf diese Weise ist eine dezentrale Konfiguration und Überwachung der Standard- und Sicherheitsgeräte im Netzwerk möglich. Bei Verwendung einer DeviceNet-Schnittstellenkarte im Netzwerkkonfigurator-PC kann dieser direkt an das DeviceNet-Netzwerk angeschlossen werden.



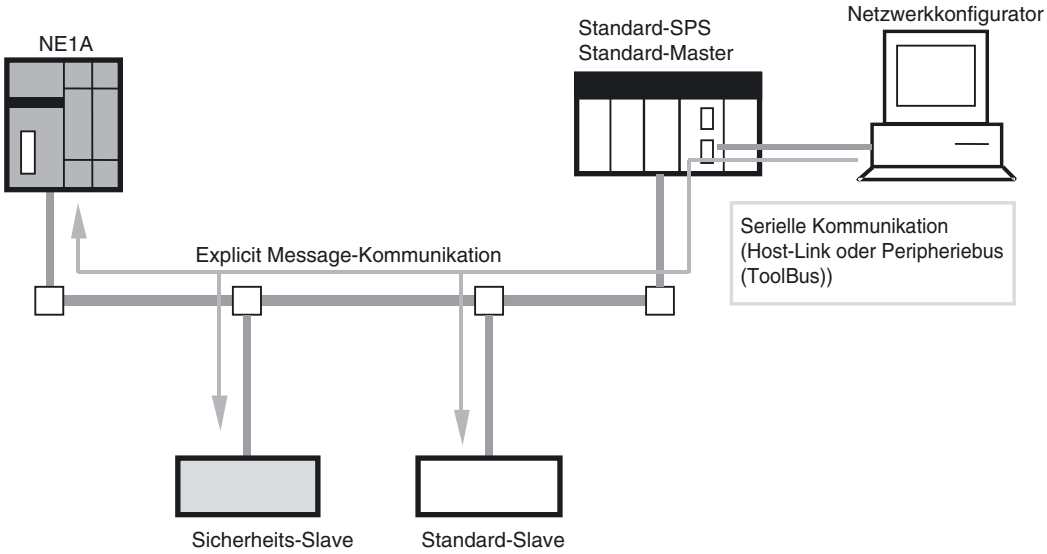
USB-Verbindung mit dem Sicherheitsnetzwerk-Controller NE1A

Der Netzwerkkonfigurator-PC kann auch direkt mit der USB-Schnittstelle des Sicherheitsnetzwerk-Controllers NE1A verbunden werden. Diese Anschlussvariante ermöglicht nicht nur die dezentrale Konfiguration und Überwachung des direkt an den Netzwerkkonfigurator-PC angeschlossenen Sicherheitsnetzwerk-Controllers NE1A, sondern auch die Konfiguration und Überwachung anderer Geräte im Netzwerk. Bei Verwendung einer USB-Verbindung benötigt der Netzwerkkonfigurator-PC keine Knotenadresse im DeviceNet-Netzwerk.



Serielle Verbindung mit einer OMRON SPS

Der Netzwerkkonfigurator-PC kann auch direkt mit der seriellen Schnittstelle einer OMRON SPS verbunden werden. Auf diese Weise ist eine dezentrale Konfiguration und Überwachung der Standard- und Sicherheitsgeräte im Netzwerk möglich. Bei einer SPS-Verbindung benötigt der Netzwerkkonfigurator keine Knotenadresse im DeviceNet-Netzwerk.

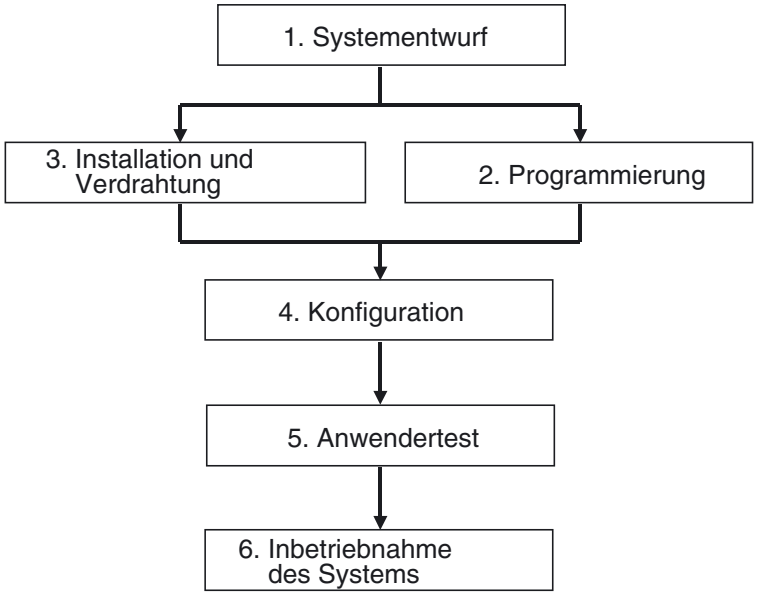


Hinweis Beim Download von einem Standard-Master zum Sicherheitsnetzwerk-Controller NE1A folgende Punkte beachten:

- Der Überwachungszeitraum für die Zeitüberschreitung des Standard-Masters muss mindestens 15 Sekunden betragen.
- Die dezentrale E/A-Kommunikation zwischen Standard-Master und NE1A muss angehalten (unterbrochen) werden.

1-3 Vorgehensweise bei der Einrichtung des Systems

Das nachstehende Diagramm skizziert die einzelnen Arbeitsschritte bis zur Inbetriebnahme des Sicherheitssystems.



Der nachstehenden Tabelle können Sie entnehmen, in welchen Kapiteln dieses Handbuchs Sie die für die einzelnen Phasen benötigten Informationen zum Sicherheitsnetzwerk-Controller NE1A finden.

Phase	Benötigte Informationen	Details
Systementwurf	• Übersicht über das System und Beispielkonfigurationen • Technische Daten und Funktionen • Leistung	Kapitel 1 Kapitel 2, 4, 5, 6, 7 und 8 Kapitel 9
Programmierung	• Richtlinien zur Programmierung • Funktionsblockspezifikationen	Kapitel 6

Installation und Verdrahtung	• Knotenadressen- und Baudrateneinstellung
	• Installationsumgebung
	• Geräteanschlüsse
	  • Verdrahtung der Spannungsversorgung
	  • Anschluss von E/A-Geräten
	  • Verdrahtung für DeviceNet
		Kapitel 4, Abschnitt 1
		Kapitel 3

Konfiguration	• Konfigurationsverfahren	Kapitel 7
Anwendertest	• Fehlerklassifizierung und Fehlerprotokoll	Kapitel 10
Betrieb des Systems	• Wartung und Inspektion	Kapitel 11

Informationen zur Installation von DeviceNet-Netzwerken, der Konstruktion von DeviceNet Safety-Systemen, der Verwendung des Netzwerkkonfigurators und anderer Programmiergeräte sowie zu anderen im Sicherheitssystem eingesetzten Geräten finden Sie in den in der nachstehenden Tabelle aufgeführten Handbüchern.

Parameter	Titel des Handbuchs	Cat. No.
Installation von DeviceNet-Netzwerken	DeviceNet-Bedienerhandbuch	W379
Konstruktion von DeviceNet Safety-Systemen	DeviceNet Safety System Konfigurationshandbuch	Z905
Verwendung des Netzwerkkonfigurators		
Verwendung anderer Programmiergeräte		
Installation von Sicherheits-E/A-Modulen	Bedienerhandbuch für DeviceNet Safety Sicherheits-E/A-Module	Z904

ABSCHNITT 2
Technische Daten und Bezeichnungen

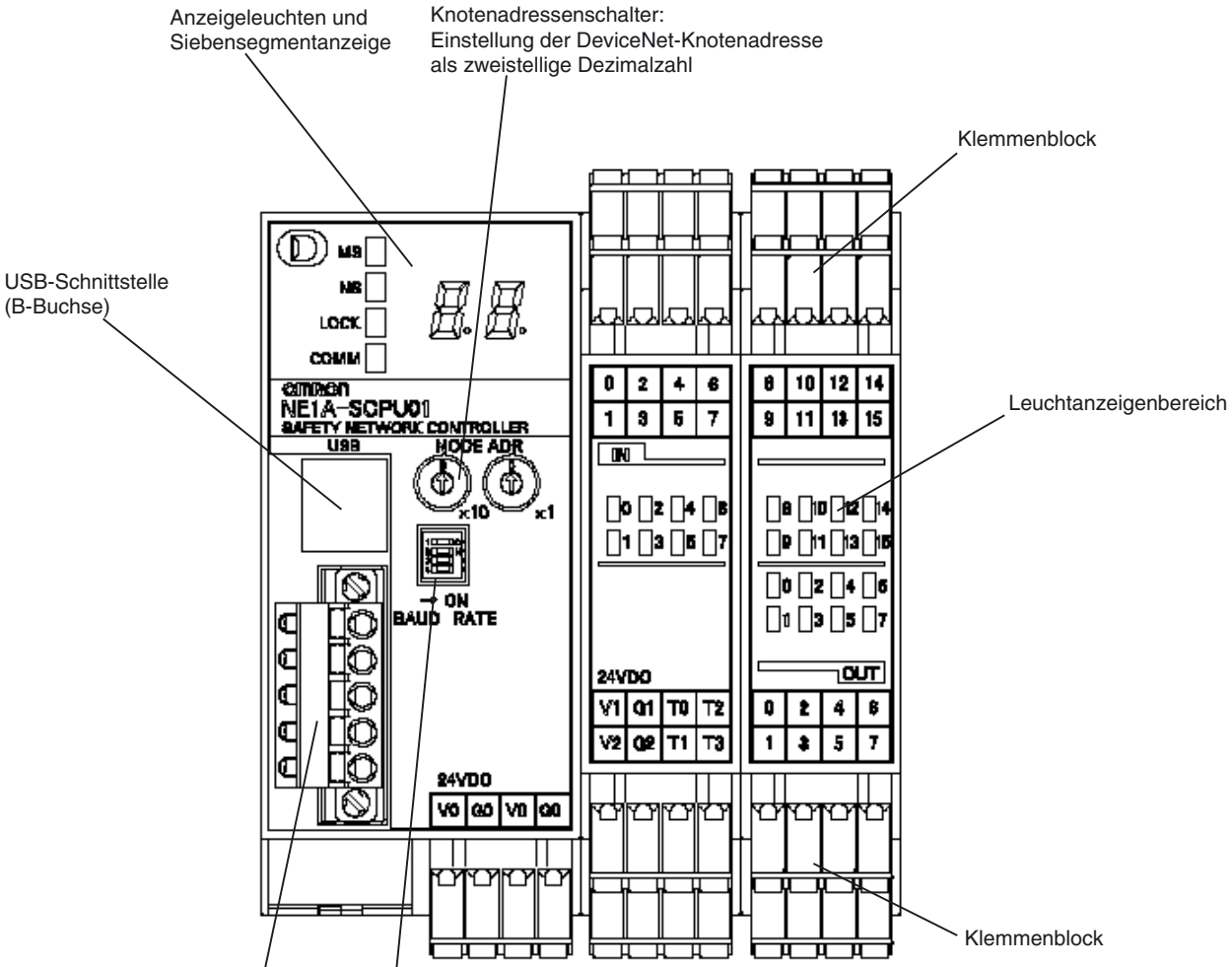
2-1 Bezeichnungen der Komponenten, Anzeigen und Bedienelemente 18
2-1-1 Bezeichnungen 18
2-1-2 Kontrollleuchten und Anzeigen 21
2-1-3 Schaltereinstellungen 23
2-1-4 DeviceNet-Stecker 24
2-1-5 USB-Buchse 24
2-1-6 Eingangs- und Ausgangsklemmen und interne Verbindungen 25
2-2 Technische Daten 27
2-2-1 Allgemeine technische Daten 27
2-2-2 DeviceNet-Kommunikationsspezifikationen 29
2-2-3 E/A-Spezifikationen 30

2-1 Bezeichnungen der Komponenten, Anzeigen und Bedienelemente

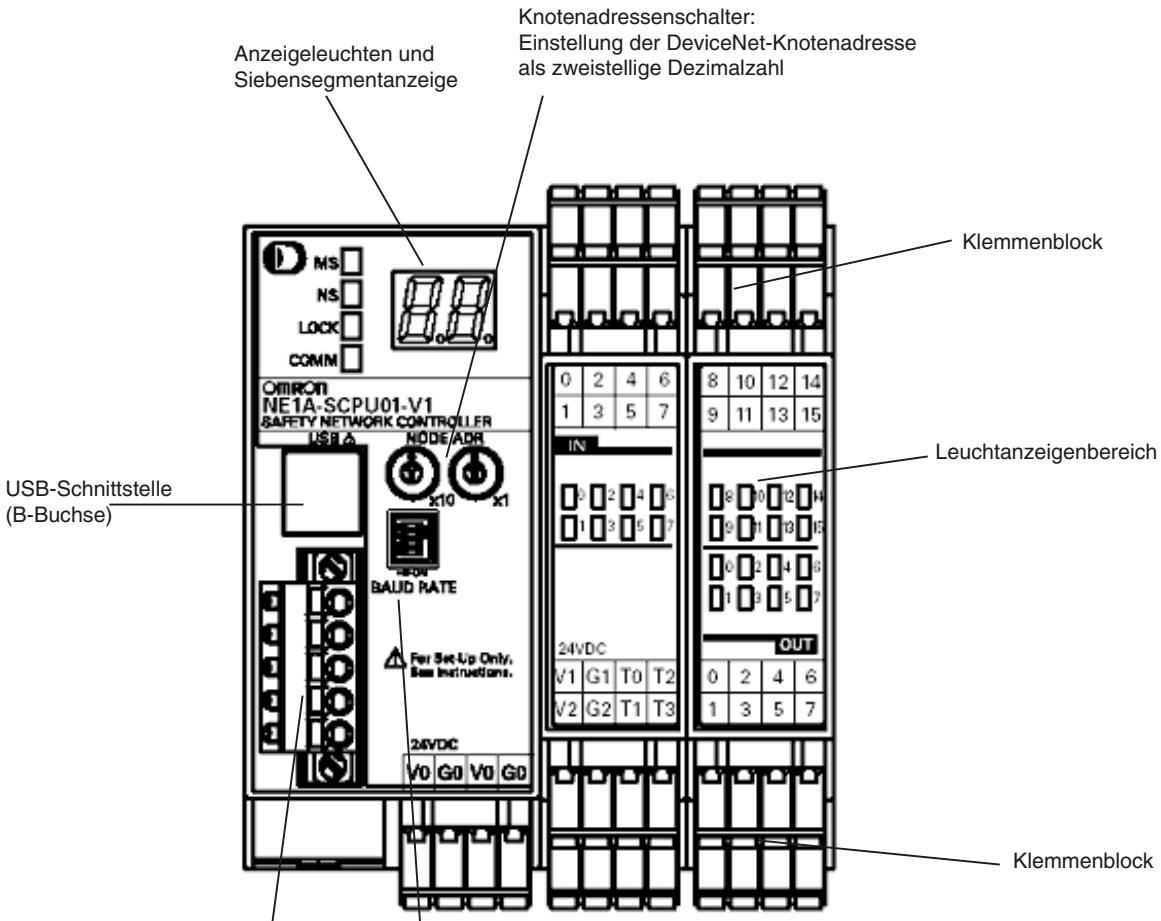
Dieser Abschnitt beschreibt die Komponenten, Anzeigen und Bedienelemente des Sicherheitsnetzwerk-Controllers NE1A.

2-1-1 Bezeichnungen

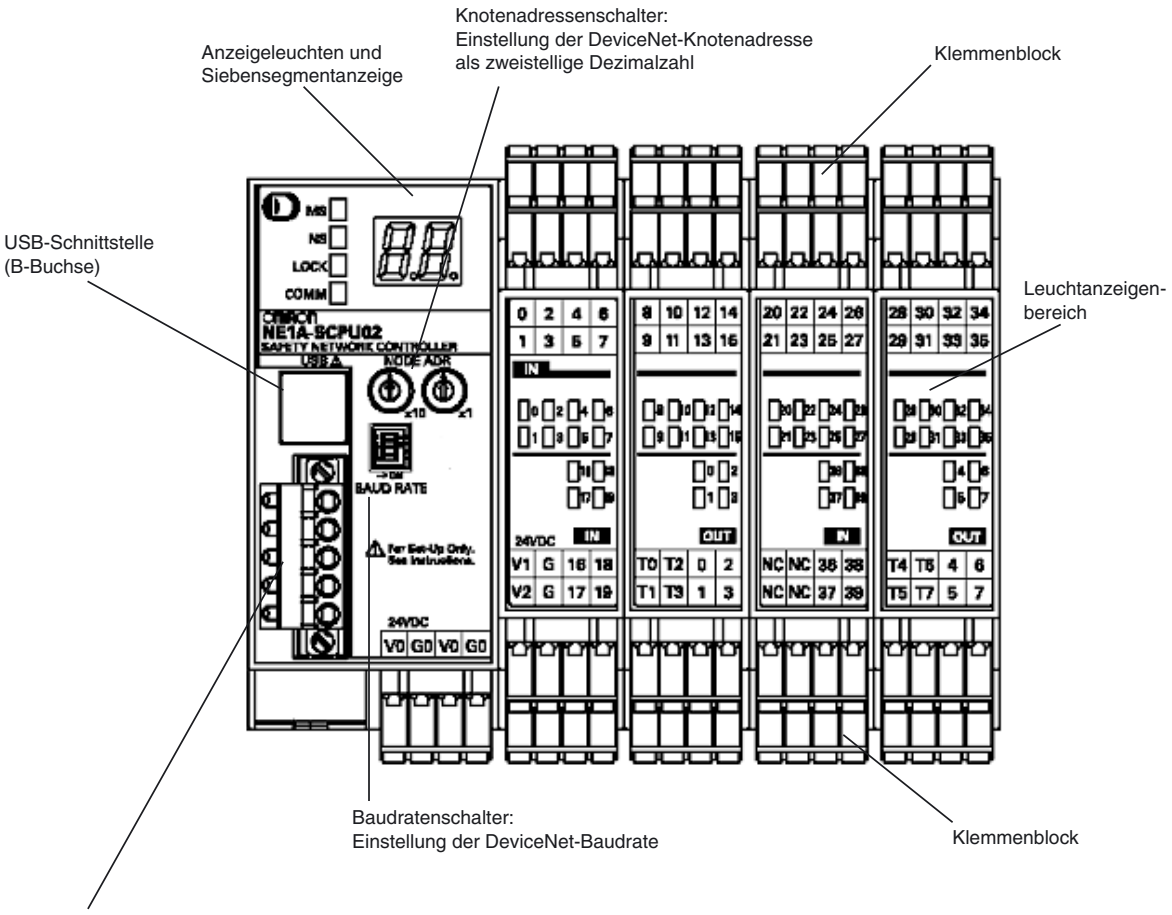
NE1A-SCPU01 (vor Version 1.0)



NE1A-SCPU01 (ab Geräteversion 1.0)



NE1A-SCPU02


Anzeigeleuchten und Siebensegmentanzeige
Knotenadressenschalter: Einstellung der DeviceNet-Knotenadresse als zweistellige Dezimalzahl
Klemmenblock
USB-Schnittstelle (B-Buchse)
Leuchtanzeigen-bereich
MS
NS
LOCK
COMM
OMRON
NE1A-SCPU02
SAFETY NETWORK CONTROLLER
USB
NODE ADR
BAUD RATE
24VDC
V0 G0 V0 G0
Baudratenschalter: Einstellung der DeviceNet-Baudrate
Klemmenblock
DeviceNet-Buchse: Die Spannungsversorgung des Netzwerks erfolgt ebenfalls über diese Buchse. Anschlussmöglichkeit für das Netzwerkkommunikationskabel. Bestellbezeichnung des passenden Steckers: XW4B-05C1-H1-D

2-1-2 Kontrollleuchten und Anzeigen

Statusanzeigen

Die folgenden LED-Anzeigen geben Aufschluss über den Status des Sicherheitsnetzwerk-Controllers NE1A, des Netzwerks und der E/A-Punkte.

- MS (Baugruppenstatus)
- NS (Netzwerkstatus)
- LOCK (Konfigurationsschutz)
- COMM (USB-Kommunikationsstatus)
- IN 0 bis 15 (Status der lokalen Eingänge, NE1A-SCPU01(-V1))
- IN 0 bis 39 (Status der lokalen Eingänge, NE1A-SCPU02)
- OUT 0 bis 7 (Status der lokalen Ausgänge)

Bezeichnung der LED-Anzeige	Farbe	Status	Bedeutung
MS (Baugruppenstatus)	Grün	☐	Normalbetrieb
		◪	Leerlauf
	Rot	☐	Kritischer Fehler
		◪	Abbruch
	Grün/Rot	◪	Selbstdiagnose, Warten auf TUNID-Einstellung oder Warten auf Konfiguration
	-	■	Versorgungsspannung ausgeschaltet
NS (Netzwerkstatus)	Grün	☐	Online-Verbindung besteht
		◪	Online-Verbindung besteht nicht
	Rot	☐	Kommunikation nicht möglich
		◪	E/A-Kommunikationsfehler
	Grün/Rot	◪	Warten auf TUNID-Einstellung
	-	■	Nicht online oder DeviceNet-Kommunikation deaktiviert (Standalone-Controller-Modus)
LOCK (Konfigurationsschutz)	Gelb	☐	Die Konfiguration ist gültig und geschützt
		◪	Die Konfiguration ist gültig und nicht geschützt
		■	Die Konfiguration ist ungültig
COMM (USB)	Gelb	◪	Aktuelle Datenübertragung
		■	Keine aktuelle Datenübertragung
NE1A-SCPU01 IN 0, 1, 2, …15 OUT 0, 1, 2, …7 (Status der lokalen E/A) NE1A-SCPU02 IN 0, 1, 2 …39 OUT 0, 1, 2, …7 (Status der lokalen E/A)	Gelb	☐	E/A-Signal ist EIN
	Rot	☐	Fehler in den E/A-Schaltkreisen entdeckt. Diskrepanzfehler bei einem im Zweikanalmodus betriebenen Eingang aufgetreten. Diskrepanzfehler bei einem im Zweikanalmodus betriebenen Ausgang aufgetreten.
		◪	Fehler im E/A-Schaltkreis des anderen zu diesem im Zweikanalmodus betriebenen Ein- bzw. Ausgang gehörenden Ein- bzw. Ausgangs gefunden (dieser E/A-Schaltkreis ist fehlerfrei).
	-	■	E/A-Signal ist AUS

☐ : Leuchtet ◪ : Blinkt ■ : AUS

Siebensegmentanzeige

Im normalen Betrieb zeigt die Siebensegmentanzeige die Knotenadresse des Sicherheitsnetzwerk-Controller NE1A. Im Fehlerfall zeigt sie abwechselnd den Fehlercode und die Knotenadresse des Geräts, bei dem der Fehler auftrat. Ist die DeviceNet-Kommunikation deaktiviert (Standalone-Controller-Modus), zeigt die Siebensegmentanzeige im normalen Betrieb „nd“.

Status		Anzeige	
Normaler Betrieb, DeviceNet-Kommunikation aktiviert	Betriebsmodus: RUN Sicherheits-E/A-Kommunikation: in Betrieb oder nicht eingerichtet	Knotenadresse des Sicherheitsnetzwerk-Controllers NE1A (00 bis 63)	Leuchtet
	Betriebsmodus: RUN Sicherheits-E/A-Kommunikation: Nicht in Betrieb		Blinkt
	Betriebsmodus: Selbsttest, konfigurierend oder Leerlauf		Blinkt
Normaler Betrieb, DeviceNet-Kommunikation deaktiviert	Betriebsmodus: RUN	„nd“	Leuchtet
	Betriebsmodus: Selbsttest, konfigurierend oder Leerlauf		Blinkt
Fehlerzustände	Kritischer Fehler	Unbestimmt	
		Nur Fehlercode	Leuchtet
	Abbruch	Nur Fehlercode	Leuchtet
	Geringfügiger Fehler	Abwechselnd Fehlercode und die Knotenadresse des Geräts, bei dem der Fehler auftrat	

⚠ VORSICHT

Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden,

dürfen die Anzeigen des Sicherheitsnetzwerk-Controllers NE1A nicht für Sicherheitsfunktionen benutzt werden.

Hinweis Die Anzeige von Fehlern erfolgt durch entsprechende Kombinationen der LED-Anzeigen „MS“ und „NS“ und der Siebensegmentanzeige. Detailinformationen zur Bedeutung dieser Kombinationen finden Sie in *Kapitel 10: Fehlersuche.*

2-1-3 Schaltereinstellungen

Knotenadressenschalter

Die Einstellung der Knotenadresse erfolgt mithilfe der Drehschalter an der Front des Sicherheitsnetzwerk-Controllers NE1A.

Einstellverfahren	Zweistellige Dezimalzahl
Bereich	0 bis 63

Hinweis Ab Werk ist die Knotenadresse auf 63 eingestellt.

Die Knotenadresse kann auf einen beliebigen Wert innerhalb des zulässigen Bereichs eingestellt werden, sofern diese Adresse nicht von einem anderen Knoten verwendet wird. Wenn die Drehschalter auf einen Wert zwischen 64 und 99 eingestellt sind, kann die Einstellung der Knotenadresse durch eine Softwareeinstellung des Netzwerkkonfigurators erfolgen.

WICHTIG

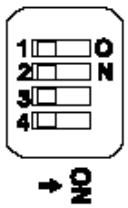
- Schalten Sie vor dem Einstellen der Drehschalter die Versorgungsspannung des Sicherheitsnetzwerk-Controllers NE1A aus.
- Bei eingeschalteter Spannungsversorgung darf die Einstellung der Drehschalter nicht geändert werden. Erfolgt eine Änderung der Einstellungen bei eingeschalteter Spannungsversorgung, erkennt der Sicherheitsnetzwerk-Controller NE1A dies als Konfigurationsänderung und geht in den Sperr-Zustand über.
- Wurde für mehrere Knoten dieselbe Knotenadresse eingestellt, tritt ein Knotenadressen-Mehrfachverwendungs-Fehler auf. In diesem Fall findet keine Kommunikation im Netzwerk statt.

Hinweis

- Verwenden Sie zum Einstellen der Drehschalter einen kleinen Schlitzschraubendreher. Achten Sie darauf, die Drehschalter nicht zu beschädigen.
- Hinweise zum Konfigurieren der Software finden Sie unter *4-1 Anfangskonfiguration*.

Baudratenschalter

Die Einstellung der DeviceNet-Baudrate erfolgt mithilfe der DIP-Schalter an der Front des Sicherheitsnetzwerk-Controllers NE1A. Die folgende Tabelle zeigt die Schaltereinstellungen für die möglichen Baudraten.



DIP-Schalter				Baudrate
1	2	3	4	
AUS	AUS	AUS	AUS	125 kBit/s
EIN	AUS	AUS	AUS	250 kBit/s
AUS	EIN	AUS	AUS	500 kBit/s
EIN	EIN	AUS	AUS	Softwareeinstellung
ON oder OFF	ON oder OFF	EIN	AUS	
ON oder OFF	ON oder OFF	ON oder OFF	EIN	Automatische Erkennung der Baudrate

Hinweis Ab Werk ist die Baudrate auf 125 kBit/s eingestellt.

Hinweis Hinweise zum Konfigurieren der Software finden Sie unter *4-1 Anfangskonfiguration*.

2-1-4 DeviceNet-Stecker

Die Kontakte des DeviceNet-Steckers tragen eine Farbkodierung, die der des DeviceNet-Kommunikationskabels entspricht. Achten Sie beim Anschluss des Kabels an den Stecker auf die Übereinstimmung zwischen Kontaktfarbe und Adernfarbe:

Farbe	Beschreibung
Rot	V+
Weiß	Signal (CAN H)
-	Drain
Blau	Signal (CAN L)
Schwarz	V−

Weitere Einzelheiten über Kommunikationsspezifikationen und Verdrahtung finden Sie im *DeviceNet-Bedienerhandbuch* (W379).

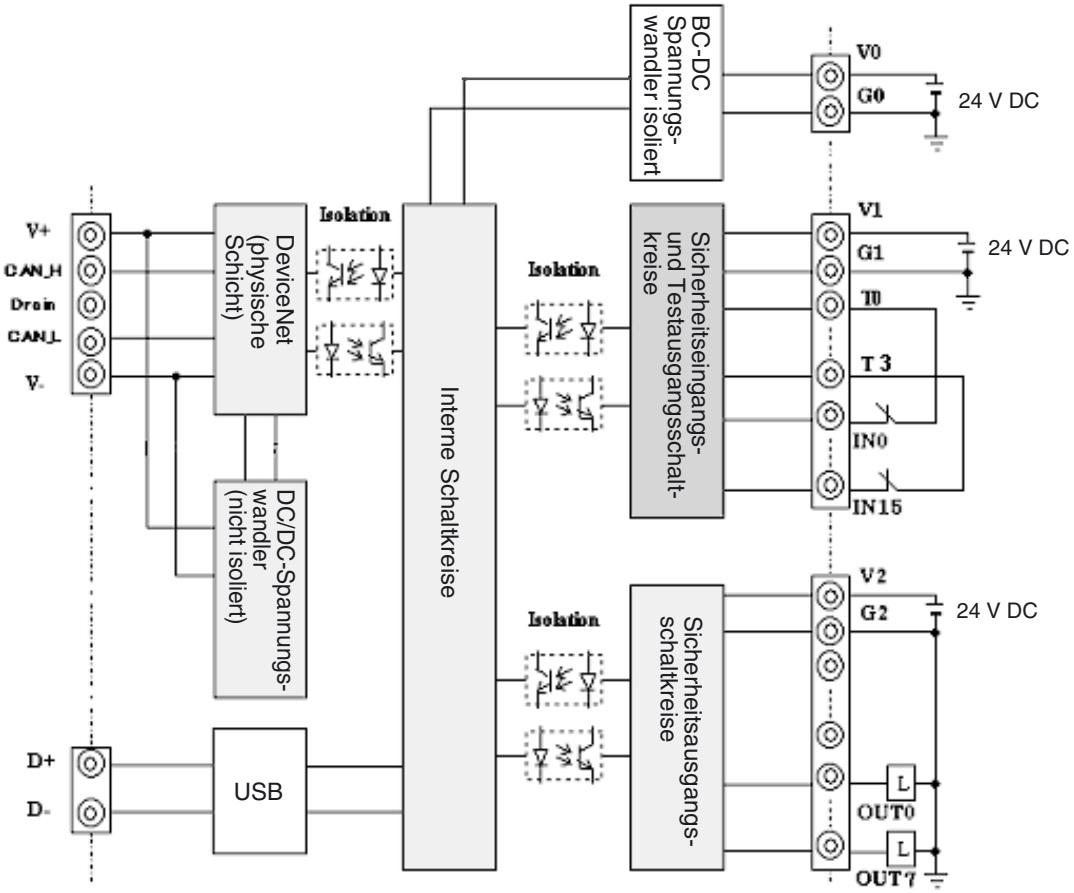
WICHTIG Schalten Sie vor Beginn der Arbeiten für die DeviceNet-Verdrahtung die Versorgungsspannung des Sicherheitsnetzwerk-Controllers NE1A und aller Netzwerkteilnehmer und Kommunikationsleitungen aus.

2-1-5 USB-Buchse

Die USB-Buchse ermöglicht den direkten Anschluss des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 an einen PC (z. B. bei Verwendung als Standalone-Controller) für die Konfiguration mithilfe des Netzwerkkonfigurators. Der Sicherheitsnetzwerk-Controller NE1A unterstützt den USB-Standard 1.1. Verwenden Sie für die USB-Verbindung ein handelsübliches USB-A zu USB-B-Kabel (männlich/männlich).

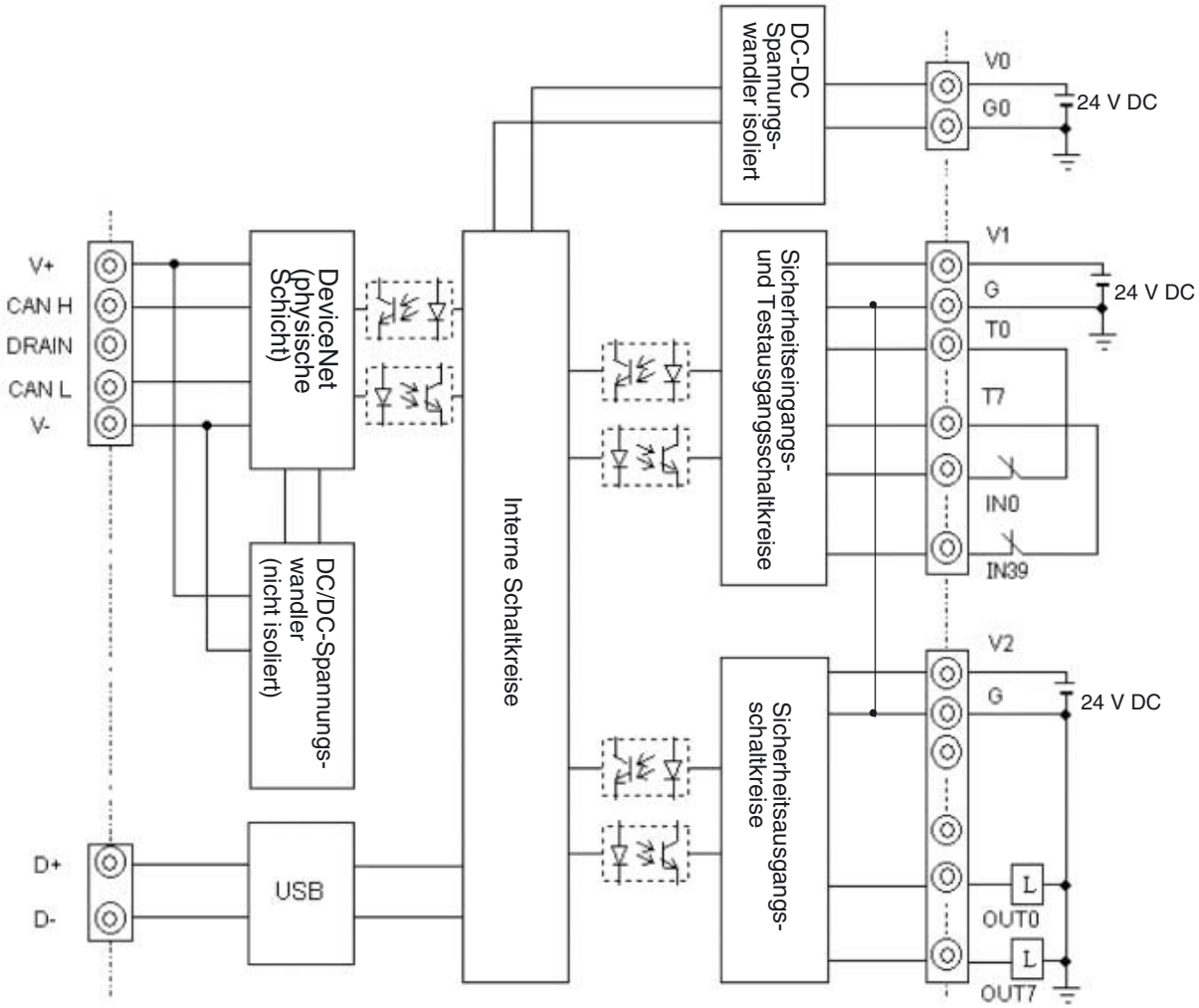
2-1-6 Eingangs- und Ausgangsklemmen und interne Verbindungen

NE1A-SCPU01(-V1)



Klemmenbezeichnung	Beschreibung
V0	Versorgungsspannung (+ 24 V DC) für die internen Schaltkreise Die beiden mit V0 bezeichneten Klemmen sind intern miteinander verbunden.
G0	Versorgungsspannung (0 V) für die internen Schaltkreise Die beiden mit G0 bezeichneten Klemmen sind intern miteinander verbunden.
V1	Spannungsversorgungsklemme (+24 V DC) für externe Eingangsgeräte und Testausgänge
G1	Spannungsversorgungsklemme (0 V) für externe Eingangsgeräte und Test-ausgänge
V2	Spannungsversorgungsklemme (+ 24 V DC) für externe Ausgangsgeräte
G2	Spannungsversorgungsklemme (0 V) für externe Ausgangsgeräte
IN0 bis IN15	Sicherheitseingangsklemmen
T0 bis T3	Testausgangsklemmen (werden über ein Schaltgerät mit einem der Sicher-heitseingänge verbunden). An jeder Testausgangsklemme wird ein eindeuti-ges (unterschiedliches) Testimpulsmuster ausgegeben. Klemme T3 unterstützt auch eine Stromüberwachungsfunktion für das Ausgangssignal (beispielsweise für eine Muting-Lampe).
OUT0 bis OUT7	Sicherheitsausgangsklemmen

NE1A-SCPU02-V1



Klemmen-bezeichnung	Beschreibung
V0	Versorgungsspannung (+24 V DC) für die internen Schaltkreise Die beiden mit V0 bezeichneten Klemmen sind intern miteinander verbunden.
G0	Versorgungsspannung (0 V) für die internen Schaltkreise Die beiden mit G0 bezeichneten Klemmen sind intern miteinander verbunden.
V1	Spannungsversorgungsklemme (+24 V DC) für externe Eingangsgeräte und Testausgänge
G	Spannungsversorgungsklemme (0 V) für externe Eingangsgeräte und Testausgänge
V2	Spannungsversorgungsklemme (+ 24 V DC) für externe Ausgangsgeräte
G	Spannungsversorgungsklemme (0 V) für externe Ausgangsgeräte
IN0 bis IN39	Sicherheitseingangsklemmen
T0 bis T3	Testausgangsklemmen (werden über ein Schaltgerät mit einem der Sicherheitseingänge verbunden). An jeder Testausgangsklemme wird ein eindeutiges (unterschiedliches) Testimpulsmuster ausgegeben. Klemme T3 unterstützt auch eine Stromüberwachungs-funktion für das Ausgangssignal (beispielsweise für eine Muting-Lampe).
T4 bis T7	Testausgangsklemmen (werden über ein Schaltgerät mit einem der Sicherheitseingänge verbunden). An jeder Testausgangsklemme wird ein eindeutiges (unterschiedliches) Testimpulsmuster ausgegeben. Klemme T7 unterstützt auch eine Stromüberwachungsfunk-tion für das Ausgangssignal (beispielsweise für eine Muting-Lampe).
OUT0 bis OUT7	Sicherheitsausgangsklemmen

2-2 Technische Daten

Dieser Abschnitt enthält die technischen Daten des Sicherheitsnetzwerk-Controllers NE1A.

2-2-1 Allgemeine technische Daten

NE1A-SCPU01(-V1)

Parameter		Technische Daten
DeviceNet-Versorgungsspannung		11 bis 25 V DC (Von der DeviceNet-Buchse)
Baugruppen-Versorgungsspannung V0 (siehe Hinweis)		20,4 bis 26,4 V DC (24 V DC -15 % / +10 %)
E/A-Versorgungsspannungen V1 und V2 (siehe Hinweis)		20,4 bis 26,4 V DC (24 V DC -15 % / +10 %)
Stromaufnahme	DeviceNet	15 mA bei 24 V DC
	Interne Logikschaltkreise	230 mA bei 24 V DC
Überspannungskategorie		II (IEC 61131-2: 4.4.2)
EMV		Entspricht IEC 61131-2
Vibrationsfestigkeit		0,35 mm bei 10 bis 57 Hz, 50 m/s^2 bei 57 bis 150 Hz
Stoßfestigkeit		150 m/s^2 für 11 ms
Montage		DIN-Schiene (TH35-7.5/TH35-15 gemäß IEC 60715)
Temperatur (Betrieb)		−10 bis 55°C
Luftfeuchtigkeit		10 % bis 95 % (ohne Kondensation)
Temperatur (Lagerung)		−40 bis 70°C
Schutzklasse		IP20
Serielle Schnittstelle		USB Ver. 1.1
Gewicht		460 g

Hinweis V0 und G0: Versorgungsspannung für die internen Logikschaltkreise / V1 und G1: Versorgungsspannung für externe Eingangsgeräte und Testausgänge / V2 und G2: Versorgungsspannung für externe Ausgangsgeräte

NE1A-SCPU02

Parameter		Technische Daten
DeviceNet-Versorgungsspannung		11 bis 25 V DC (Von der DeviceNet-Buchse)
Baugruppen-Versorgungsspannung V0 (siehe Hinweis)		20,4 bis 26,4 V DC (24 V DC -15 % / +10 %)
E/A-Versorgungsspannungen V1 und V2 (siehe Hinweis)		20,4 bis 26,4 V DC (24 V DC -15 % / +10 %)
Stromauf-nahme	DeviceNet	15 mA bei 24 V DC
	Interne Logikschaltkreise	280 mA bei 24 V DC
Überspannungskategorie		II (IEC 61131-2: 4.4.2)
EMV		Entspricht IEC 61131-2
Vibrationsfestigkeit		0,35 mm bei 10 bis 57 Hz, 50 m/s^2 bei 57 bis 150 Hz
Stoßfestigkeit		150 m/s^2 für 11 ms
Montage		DIN-Schiene (TH35-7.5/TH35-15 gemäß IEC 60715)
Temperatur (Betrieb)		–10 bis 55°C
Luftfeuchtigkeit		10 % bis 95 % (ohne Kondensation)
Temperatur (Lagerung)		–40 bis 70°C
Schutzklasse		IP20
Serielle Schnittstelle		USB Ver. 1.1
Gewicht		690 g

Hinweis V0 und G0: Versorgungsspannung für die internen Logikschaltkreise / V1 und G: Versorgungsspannung für externe Eingangsgeräte und Testausgänge
V2 und G: Versorgungsspannung für externe Ausgangsgeräte
G von V1 und G von V2 sind intern miteinander verbunden.

2-2-2 DeviceNet-Kommunikationsspezifikationen

<table>
<tr><th>Parameter</th><th colspan="4">Technische Daten</th></tr>
<tr><td>Kommunikations-protokoll</td><td colspan="4">Entspricht DeviceNet.</td></tr>
<tr><td>Anschlussart</td><td colspan="4">Multidrop- und T-Abzweiganschlüsse sind kombinierbar (für Hauptleitung und Abzweigleitungen).</td></tr>
<tr><td>Baudrate</td><td colspan="4">500 kBit/s, 250 kBit/s, 125 kBit/s</td></tr>
<tr><td>Datenübertragungsmedium</td><td colspan="4">Fünfadriges Spezialkabel (2 Datenleitungen, 2 Versorgungsleitungen, 1 Abschirmung)</td></tr>
<tr><td rowspan="5">Entfernung für Datenübertragung</td><td>Baudrate</td><td>Maximale Netzwerklänge</td><td>Abzweiglänge</td><td>Gesamtlänge</td></tr>
<tr><td>500 kBit/s</td><td>max. 100 m (max. 100 m)</td><td>(max. 6 m)</td><td>(max. 39 m)</td></tr>
<tr><td>250 kBit/s</td><td>max. 250 m (max. 100 m)</td><td>(max. 6 m)</td><td>(max. 78 m)</td></tr>
<tr><td>125 kBit/s</td><td>max. 500 m (max. 100 m)</td><td>(max. 6 m)</td><td>(max. 156 m)</td></tr>
<tr><td colspan="4">Die Längenangaben in Klammern beziehen sich auf die Verwendung eines dünnen Kabels.</td></tr>
<tr><td>Kommunikations-Spannungsversorgung</td><td colspan="4">11 bis 25 V DC</td></tr>
<tr><td>Angeschlossene Knoten</td><td colspan="4">max. 63 Knoten</td></tr>
<tr><td>Sicherheits-E/A-Kommunikation (Controller vor Version 1.0)</td><td colspan="4">Sicherheits-Master-Funktion:
• Maximale Anzahl von Verbindungen: 16
• Maximale Datengröße: 16 Bytes Eingabedaten oder 16 Bytes Ausgabedaten (je Verbindung)
• Verbindungsart: Single-Cast, Multi-Cast
Sicherheits-Slave-Funktionen:
• Maximale Anzahl von Verbindungen: 4
• Maximale Datengröße: 16 Bytes Eingabedaten oder 16 Bytes Ausgabedaten (je Verbindung)
• Verbindungsart: Single-Cast, Multi-Cast</td></tr>
<tr><td>Sicherheits-E/A-Kommunikation (Controller ab Version 1.0)</td><td colspan="4">Sicherheits-Master-Funktion:
• Maximale Anzahl von Verbindungen: 32
• Maximale Datengröße: 16 Bytes Eingabedaten oder 16 Bytes Ausgabedaten (je Verbindung)
• Verbindungsart: Single-Cast, Multi-Cast
Sicherheits-Slave-Funktionen:
• Maximale Anzahl von Verbindungen: 4
• Maximale Datengröße: 16 Bytes Eingabedaten oder 16 Bytes Ausgabedaten (je Verbindung)
• Verbindungsart: Single-Cast, Multi-Cast</td></tr>
<tr><td>Standard-E/A-Kommunikation</td><td colspan="4">Standard-Slave-Funktion
• Maximale Anzahl von Verbindungen: 2
• Maximale Datengröße: 16 Bytes Eingabedaten und/oder 16 Bytes Ausgabedaten (je Verbindung)
• Verbindungsart: Poll, Bitstrobe, COS, Cyclic</td></tr>
<tr><td>Message-Kommunikation</td><td colspan="4">Maximale Message-Länge: 552 Byte</td></tr>
</table>

2-2-3 E/A-Spezifikationen

Sicherheitseingänge

Parameter	Technische Daten
Input type	Transistoreingang (PNP)
EIN-Spannung	min. 11 V DC zwischen der Eingangsklemme und G
AUS-Spannung	max. 5 V DC zwischen der Eingangsklemme und G
AUS-Strom	max. 1 mA
Eingangsstrom	4,5 mA

Sicherheitsausgänge

Parameter	Technische Daten
Ausgangsart	Transistorausgang (PNP)
Ausgangsnennstrom	max. 0,5 A pro Ausgang
Spannungsabfall	max. 1,2 V zwischen V2 und der Ausgangsklemme
Leckstrom	max. 0,1 mA

WICHTIG Bei Verwendung eines Sicherheitsausgangs als *Sicherheitsimpulsausgang* wird beim Einschalten des Sicherheitsausgangs zur Diagnose des Ausgangsschaltkreises ein AUS-Impulssignal (Impulsdauer: 580 μs) ausgegeben. Überprüfen Sie, dass die Eingangsansprechzeit des an den Sicherheitsnetzwerk-Controller NE1A angeschlossenen Steuergeräts lang genug ist, damit dieser Ausgangsimpuls zu keinen Fehlfunktionen führt.

Testausgänge

Eigenschaft	Technische Daten
Ausgangsart	Transistorausgang (PNP)
Ausgangsnennstrom	max. 0,7 A pro Ausgang (siehe Hinweis 1 und 2)
Spannungsabfall	max. 1,2 V DC zwischen V1 und der Ausgangsklemme
Leckstrom	max. 0,1 mA

Hinweis
(1) Simultanstrom gesamt: max. 1,4 A
(T0 bis T3: NE1A-SPCPU01(-V1), T0 bis T7: NE1A-SCPU02)
(2) Anschließbare externe Anzeige (T3, T7): 24 V DC, 15 bis 400 mA

ABSCHNITT 3
Installation und Verdrahtung

3-1 Installation 32
3-1-1 Anforderungen hinsichtlich Installation und Verdrahtung 32
3-1-2 Installation im Schaltschrank 33
3-1-3 Abmessungen und Gewicht 37
3-2 Verdrahtung 39
3-2-1 Allgemeine Anweisungen zur Verdrahtung 39
3-2-2 Verdrahtung der Versorgungsspannungs- und E/A-Leitungen 40
3-2-3 Anschluss von E/A-Geräten 42
3-2-4 DeviceNet-Verdrahtung 49
3-2-5 Verdrahtung des USB-Anschlusses 49

3-1 Installation

3-1-1 Anforderungen hinsichtlich Installation und Verdrahtung

Im Interesse maximaler Zuverlässigkeit und Ausnutzung der Möglichkeiten des Sicherheitsnetzwerk-Controllers NE1A sind bei Installation und Verdrahtung die nachfolgend aufgeführten Punkte zu beachten.

Installation und Lagerung

Lagern oder installieren Sie den Sicherheitsnetzwerk-Controller NE1A nicht an den folgenden Orten:

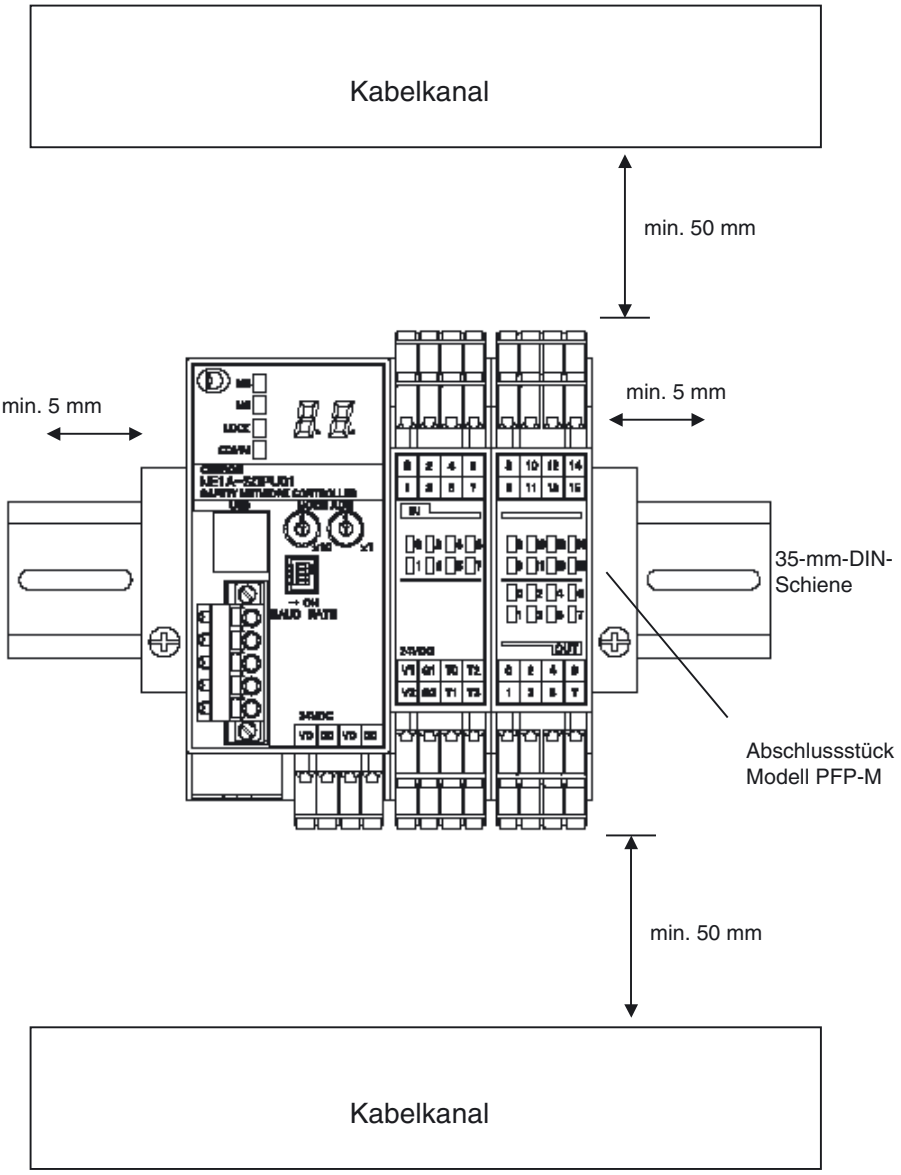
- Orte, die dem Einfluss direkter Sonneneinstrahlung ausgesetzt sind.
- Orte, an denen Temperaturen oder Luftfeuchtigkeit außerhalb der in den technischen Daten angegebenen Bereiche herrschen.
- Orte, die starken Temperaturschwankungen und damit Kondensation ausgesetzt sind.
- Orte, die dem Einfluss korrosiver oder entzündlicher Gase ausgesetzt sind.
- Orte, die dem Einfluss von Stäuben (besonders Eisenstaub) oder Salzen ausgesetzt sind.
- Orte, die dem Einfluss von Wasser, Öl oder Chemikalien ausgesetzt sind.
- Orte, die Stößen oder Schwingungen ausgesetzt sind.

Ergreifen Sie bei der Installation von Systemen an folgenden Orten angemessene und geeignete Maßnahmen. Unangemessene oder unzureichende Maßnahmen können zu Fehlfunktionen führen.

- Orte mit statischer Aufladung und anderen Störungen.
- Orte, an denen starke elektromagnetische Felder auftreten.
- Orte, die dem Einfluss von Radioaktivität ausgesetzt sein könnten.
- Orte in der Nähe von Spannungsversorgungen.

3-1-2 Installation im Schaltschrank

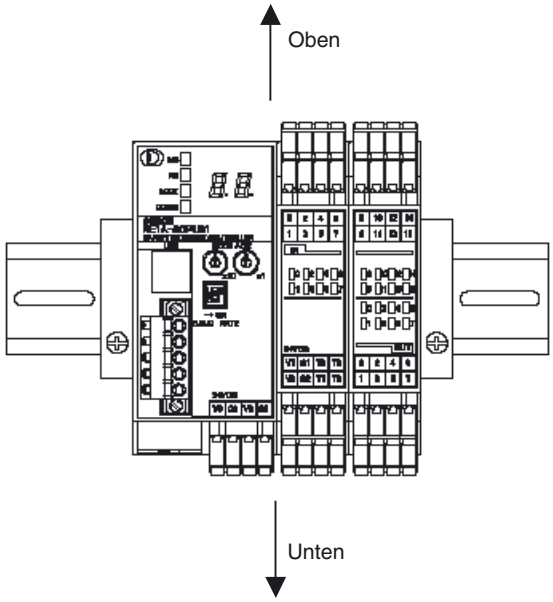
- Installieren Sie den Sicherheitsnetzwerk-Controller NE1A in einen Schaltschrank mit einer Schutzklasse von mindestens IP54 (EN60529).
- Verwenden Sie für die Installation des Sicherheitsnetzwerk-Controllers NE1A im Schaltschrank eine DIN-Schiene (TH35-7,5/TH35-15 gemäß IEC 60715). Montieren Sie den Controller mit Hilfe von PFP-M-Abschlussstücken (nicht im Lieferumfang enthalten) auf die DIN-Schiene, um sicherzustellen, dass der Sicherheitsnetzwerk-Controller bei Vibrationen nicht von der DIN-Schiene fällt.
- Lassen Sie bei der Installation des Sicherheitsnetzwerk-Controllers NE1A für Wärmeableitung und Verdrahtung einen Freiraum von mindestens 5 mm (Seiten) bzw. 50 mm (oben und unten).



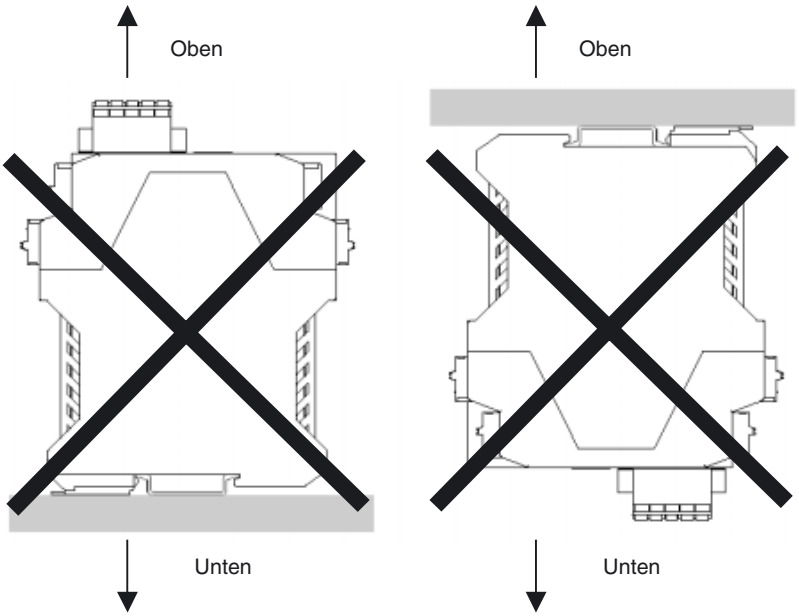
Hinweis Der Sicherheitsnetzwerk-Controller NE1A kann nur auf DIN-Schiene installiert werden und darf keinesfalls im Schaltschrank angeschraubt werden.

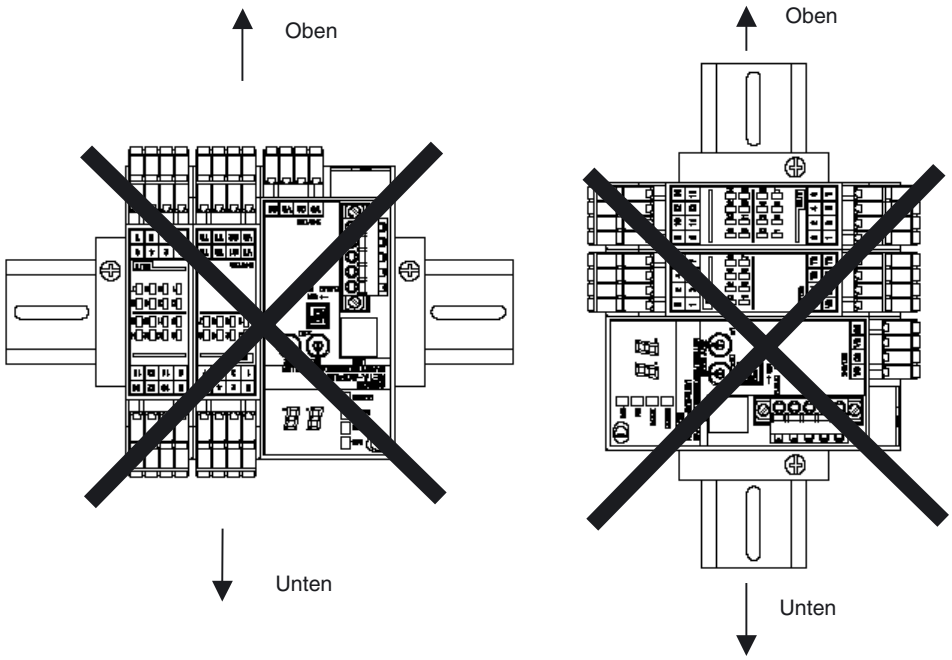
Montage

Um eine ordnungsgemäße Wärmeableitung zu gewährleisten, muss der Sicherheitsnetzwerk-Controller NE1A wie nachstehend abgebildet montiert werden.

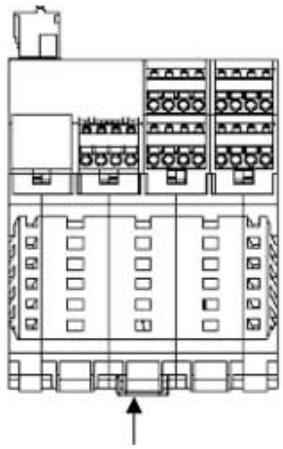


Montieren Sie den Sicherheitsnetzwerk-Controller NE1A nicht wie nachstehend abgebildet.



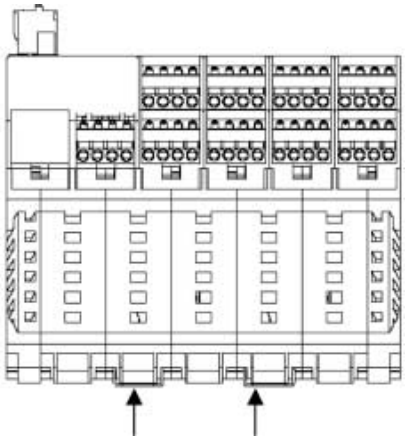

Oben
Unten
Oben
Unten

■ **Position des DIN-Schienen-Montagewinkels für Sicherheitsnetzwerk-Controller NE1A-SCPU01(-V1)**



DIN-Schienen-Montagewinkel

■ **Position der DIN-Schienen-Montagewinkel für Sicherheitsnetzwerk-Controller NE1A-SCPU02**

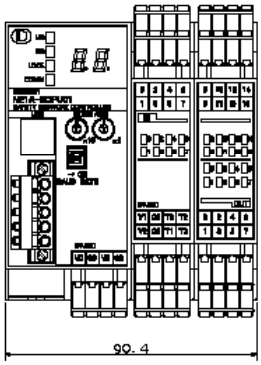


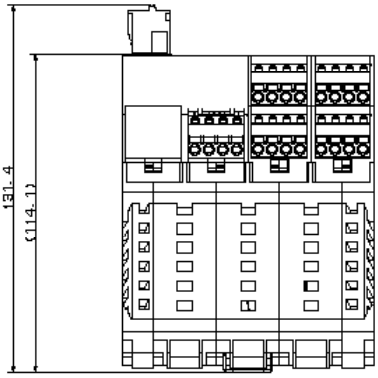
DIN-Schienen-Montagewinkel

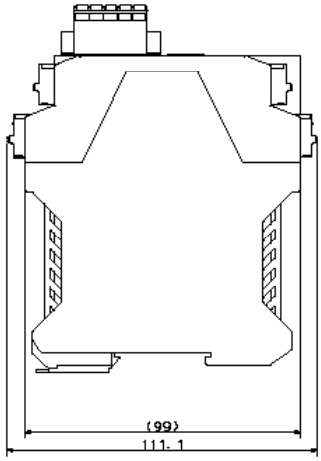
3-1-3 Abmessungen und Gewicht

Abmessungen

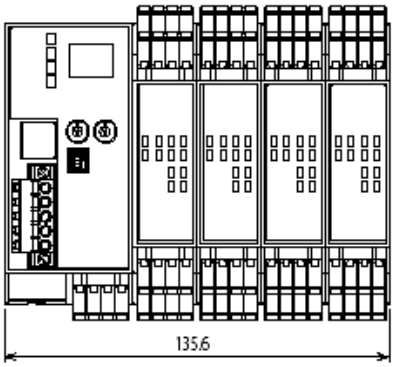
■ **NE1A-SCPU01(-V1)**

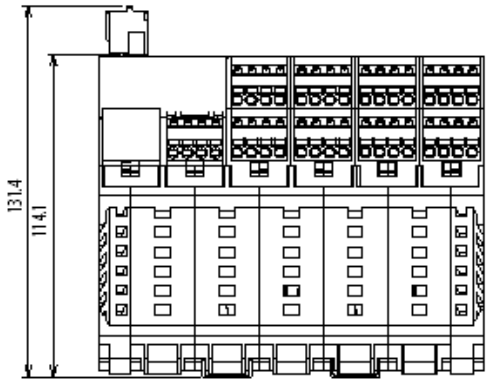


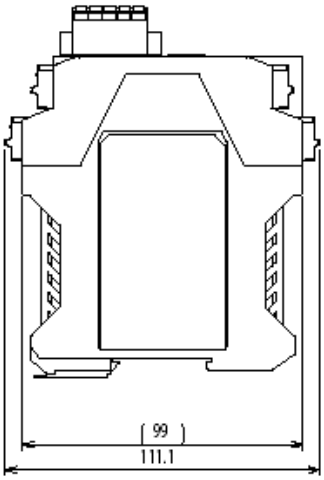




■ **NE1A-SCPU02**







Gewicht

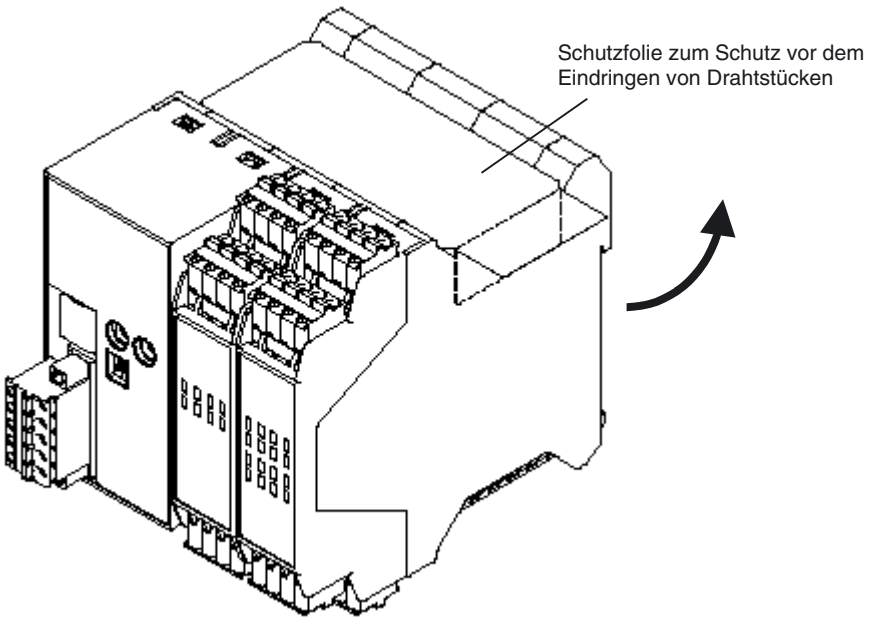
Modell	Gewicht
NE1A-SCPU01(-V1)	max. 460 g
NE1A-SCPU02	max. 690 g

3-2 Verdrahtung

3-2-1 Allgemeine Anweisungen zur Verdrahtung

Vorsichtsmaßnahmen:

- Um das Eindringen von Drahtstücken in den Sicherheitsnetzwerk-Controller NE1A zu verhindern, darf die Schutzfolie erst nach Abschluss der Verdrahtungsarbeiten abgezogen werden.
- Entfernen Sie nach Abschluss der Verdrahtungsarbeiten die Schutzfolie vom Controller, um eine ordnungsgemäße Wärmeableitung zu gewährleisten.



- Schalten Sie vor Beginn der Verdrahtungsarbeiten die Spannungsversorgung des Sicherheitsnetzwerk-Controllers NE1A aus. An den Controller angeschlossene Geräte könnten bei angeschlossener und eingeschalteter Spannungsversorgung während der Verdrahtungsarbeiten unbeabsichtigt aktiviert werden.
- Achten Sie beim Herstellen von Verbindungen an den Anschlüssen des Sicherheitsnetzwerk-Controllers NE1A darauf, Ihre Finger nicht einzuklemmen.

⚠ VORSICHT

Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, müssen die Verdrahtungsarbeiten ordnungsgemäß durchgeführt und die Funktion des Sicherheitsnetzwerk-Controllers NE1A vor Aufnahme des Betriebs überprüft werden.

3-2-2 Verdrahtung der Versorgungsspannungs- und E/A-Leitungen

Leiterquerschnitte

Drähte/Litzen für den Anschluss externer E/A-Geräte an den Sicherheitsnetzwerk-Controller NE1A müssen den in der folgenden Tabelle aufgeführten Spezifikationen genügen.

Volldraht	0,2 bis 2,5 mm^2 (AWG 24 bis AWG 12)
Litze	0,34 bis 1,5 mm^2 (AWG 22 bis AWG 16) Litzen müssen vor Verwendung mit Aderendhülsen mit isolierendem Plastikkragen nach DIN 46228-4 versehen werden.

Empfohlene Materialien und Werkzeuge

■ **Aderendhülsen mit Isolierung**

Verwenden Sie Aderendhülsen mit Isolierung (DIN 46228-4). Aderendhülsen mit ähnlichem Aussehen, die nicht DIN 46228-4 entsprechen, passen möglicherweise nicht in die Klemmen des Sicherheitsnetzwerk-Controllers NE1A. (Bei den nachfolgenden Leiterabmessungen handelt es sich ungefähre Maßangaben, die vorab bestätigt werden müssen.) Verwenden Sie für zweiadrige Aderendhülsen Litzen mit identischem Leiterquerschnitt.

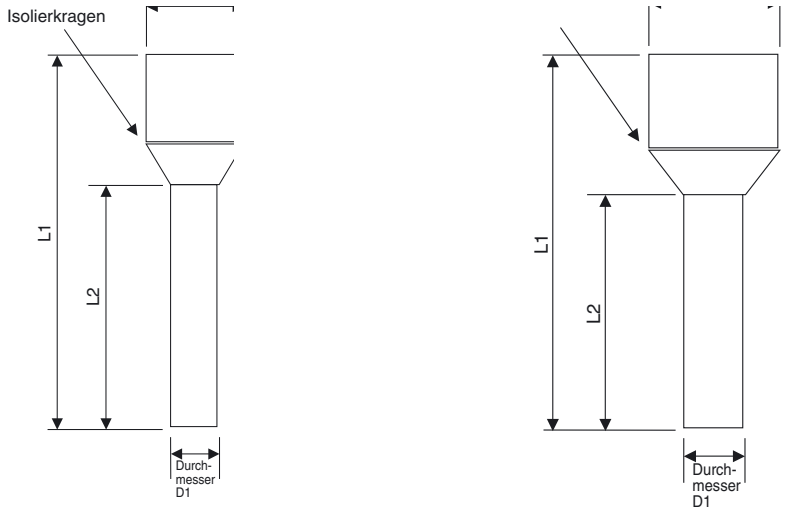
Hinweis

- Achten Sie bei der Verdrahtung mit Aderendhülsen darauf, die Endhülsen bis zum Anschlag in den Klemmenblock einzuführen.
- Verwenden Sie für zweiadrige Aderendhülsen Litzen mit identischem Leiterquerschnitt.
- Führen Sie die Aderendhülse bei Verwendung von zwei Aderendhülsen so ein, dass der Metallteil der Aderendhülse gerade im Klemmenblock sitzt, d.h. dass die Längsseiten der Isolierung vertikal ausgerichtet sind.

Spezifikationen der Aderendhülsen (Phoenix Contact)

Aderendhülsen-Typ		Leiterabmessungen		Spezifikationen der Aderendhülsen					Abmessungen
		Leiterquerschnitt (mm^2)	AWG	Länge der Abisolierung (mm)	Gesamtlänge L1 (mm)	Länge des Metallteils L2 (mm)	Innendurchmesser Kontakt D1 (mm)	Innendurchmesser Isolierkragen D2 (mm)	
Einadrige Aderendhülsen	AI 0,34-8TQ	0,34	22	10	12,5	8	0,8	2,0	*1
	AI 0,5-10WH	0,5	20	10	16	10	1,1	2,5	
	AI 0,75-10GY	0,75	18	10	16	10	1,3	2,8	
	AI 1-10RD	1,0	18	10	16	10	1,5	3,0	
	AI 1,5-10BK	1,5	16	10	18	10	1,8	3,4	
Zweiadrige Aderendhülsen	AI-TWIN 2 x 0,75-10GY	2 x 0,75	–	10	17	10	1,8	2,8/5,0	*2
	AI-TWIN 2 x 1-10RD	2 x 1	–	10	17	10	2,05	3,4/5,4	

***1: Einadrige Aderendhülse** ***2: Zweiadrige Aderendhülse**



■ **Adernendhülsenzange**

Hersteller	Modell
Phoenix Contact	CRIMPFOX UD6

Auswahl der Spannungsversorgung

Verwenden Sie eine Gleichspannungsversorgung, die die nachstehenden Anforderungen erfüllt:

- Die Gleichspannungsversorgung verwendet eine Schutzisolierung oder verstärkte Isolierung zwischen Primär- und Sekundärkreis.
- Die Gleichspannungsversorgung muss die Anforderungen für Stromkreise der Klasse 2 oder Stromkreise mit begrenzten Spannungs-/Stromwerten gemäß UL 508 erfüllen.
- Bei einem Ausfall der Versorgungsspannung muss die Ausgangsspannung für mindestens 20 ms gehalten werden.

3-2-3 Anschluss von E/A-Geräten

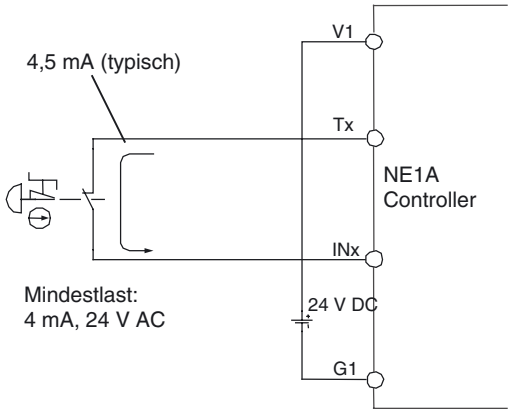
Anschluss von Eingangsgeräten

Richten Sie sich hinsichtlich der Auswahl und des Anschlusses von Eingangsgeräten nach den nachstehenden Informationen.

■ **Produkte mit mechanischen Kontaktausgängen**

Beispiele: NOT-AUS-Taster und Sicherheitspositionsschalter

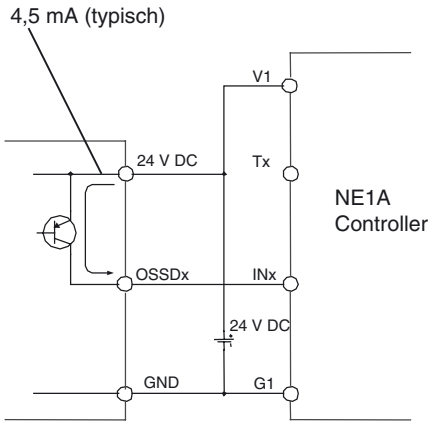
Diese Produkte können an einen Sicherheitseingang und einen Testausgang angeschlossen werden. Das vom Testausgang (Impulsausgang) des Sicherheitsnetzwerk-Controllers NE1A ausgegebene Signal wird über den Sicherheitsschalter in den Sicherheitseingang geführt.



■ **Produkte mit PNP-Transistorausgang**

Beispiel: Lichtgitter

Das Ausgangssignal des PNP-Transistorausgangs wird in den Sicherheitseingang des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 geführt.



⚠ VORSICHT

Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, müssen bei der Auswahl von Komponenten und Geräten die in der folgenden Tabelle aufgeführten Anforderungen Berücksichtigung finden.

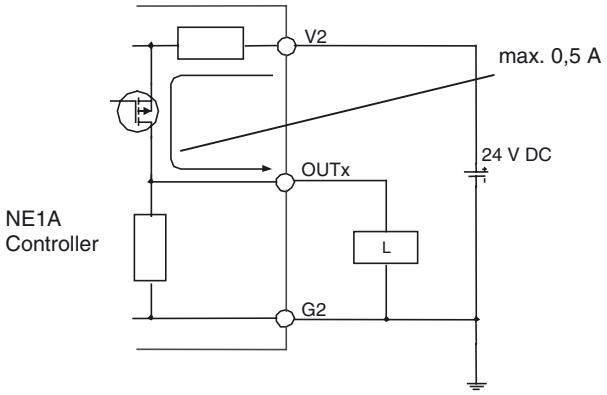
Steuerungsgerät	Anforderungen
NOT-AUS-Taster	Verwenden Sie zugelassene Schaltgeräte mit Zwangsöffnungsmechanismus gemäß IEC/EN 60947-5-1.
Verriegelungs- oder Positionsschalter für Sicherheitstüren	Verwenden Sie zugelassene Schaltgeräte mit Zwangsöffnungsmechanismus gemäß IEC/EN 60947-5-1, die Mikrolasten von 4 mA bei 24 V DC schalten können.
Sicherheitssensoren	Verwenden Sie zugelassene Schaltgeräte, die die Anforderungen der einschlägigen Produktstandards, Vorschriften und Gesetze im entsprechenden Land erfüllen.
Sicherheitsrelais mit zwangsgeführten Kontakten	Verwenden Sie zugelassene Schaltgeräte mit zwangsgeführten Kontakten, die EN 50205 entsprechen. Zu Rückführzwecken müssen Schaltgeräte mit Kontakten verwendet werden, die Mikrolasten von 4 mA bei 24 V DC schalten können.
Schütz	Verwenden Sie Schütze mit zwangsgeführten Kontakten, und überwachen Sie den Hilfsöffnerkontakt, um Ausfälle von Schützen erkennen zu können. Zur Rückführzwecken müssen Schaltgeräte mit Kontakten verwendet werden, die Mikrolasten von 4 mA bei 24 VDC schalten können.
Andere Geräte	Prüfen Sie, ob die verwendeten Geräte den Anforderungen der Steuerungskategorie entsprechen.

WICHTIG

- An den Eingängen des Sicherheitsnetzwerk-Controllers NE1A dürfen nur die spezifizierten Eingangsspannungen angelegt werden. Das Anlegen einer falschen Gleichspannung oder einer beliebigen Wechselspannung kann zu einer Beeinträchtigung der Sicherheitsfunktionen, einer Beschädigung des Sicherheitsnetzwerk-Controllers NE1A und/oder zu Bränden führen.
- Halten Sie Leitungen für E/A-Signale getrennt von Strom- oder Hochspannungsleitungen.
- Verwenden Sie E/A-Kabel von max. 30 m Länge.
- Klemmen Sie die Spannungsversorgung nicht an die Testausgänge an. Andernfalls kann das Produkt beschädigt werden; außerdem besteht Brandgefahr.

Anschluss von Ausgangsgeräten

Richten Sie sich hinsichtlich der Auswahl und des Anschlusses von Ausgangsgeräten nach den nachstehenden Informationen.



⚠ VORSICHT	
Um eine Überlastung der Ausgänge mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, dürfen keine Lasten an die Sicherheits- oder Testausgänge angeschlossen werden, die den Nennwert übersteigen.	
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, muss bei der Verdrahtung des Sicherheitsnetzwerk-Controllers NE1A sorgfältig darauf geachtet werden, dass die 24-V-DC-Leitungen nicht versehentlich oder unbeabsichtigter Weise in Kontakt mit den Sicherheits- oder Testausgängen geraten.	
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, muss der 0-V-Ausgang der Spannungsversorgung für die externen Ausgangsgeräte geerdet werden, um zu verhindern, dass die Geräte bei einem Masseschluss einer Sicherheits- oder Testausgangsleitung aktiviert werden.	
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, müssen bei der Auswahl von Komponenten und Geräten die in der folgenden Tabelle aufgeführten Anforderungen Berücksichtigung finden.	

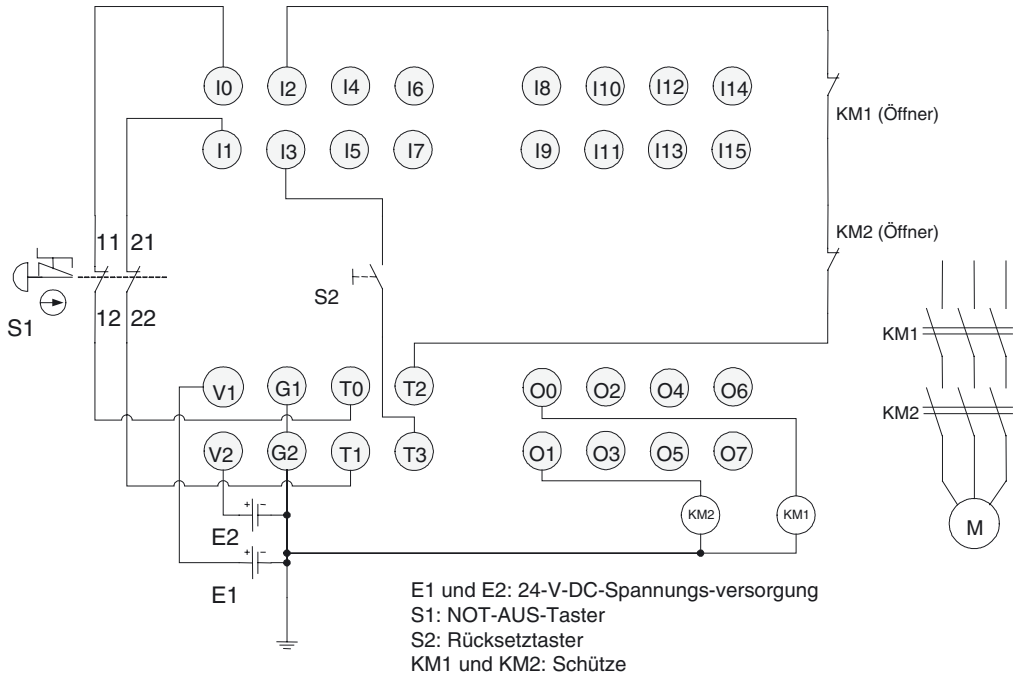
Steuerungsgerät	Anforderungen
Schütz	Verwenden Sie Schütze mit zwangsgeführten Kontakten, und überwachen Sie den Hilfsöffnerkontakt, um Ausfälle von Schützen erkennen zu können. Zur Rückführzwecken müssen Schaltgeräte mit Kontakten verwendet werden, die Mikrolasten von 4 mA bei 24 VDC schalten können.
Andere Geräte	Beurteilen Sie, ob die verwendeten Geräte den Anforderungen der Steuerungskategorie entsprechen.

WICHTIG

- Halten Sie Leitungen für E/A-Signale getrennt von Strom- oder Hochspannungsleitungen.
- Verwenden Sie E/A-Kabel von max. 30 m Länge.
- Klemmen Sie die Spannungsversorgung nicht an die Testausgänge an. Andernfalls kann das Produkt beschädigt werden; außerdem besteht Brandgefahr.

Beispiele für den Anschluss externer Geräte

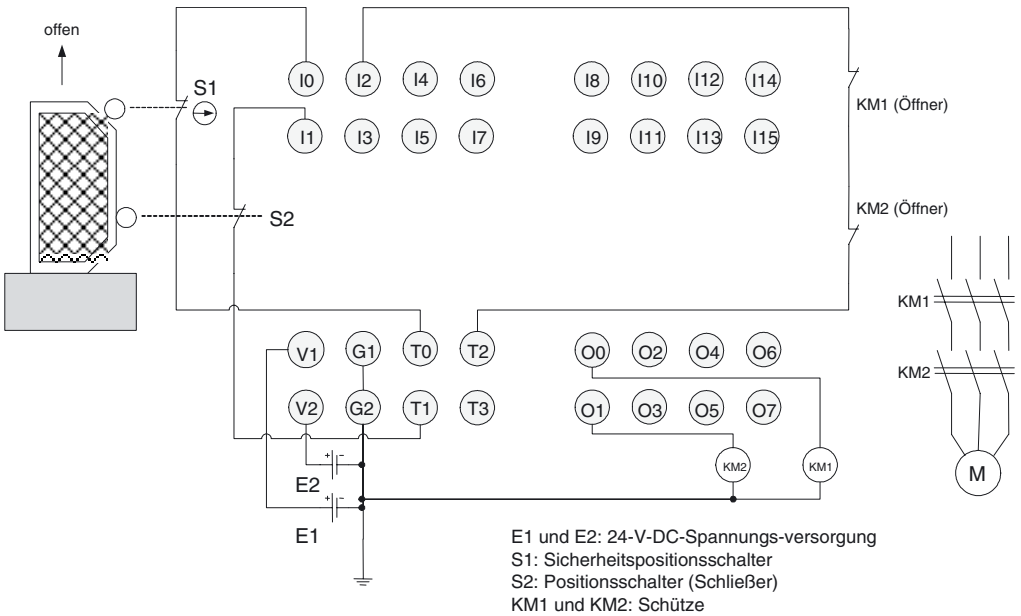
Anschluss eines NOT-AUS-Tasters



Hinweis Schließen Sie die Klemmen V0 und G0 (Spannungsversorgung für interne Schaltkreise) an eine 24-V-DC-Spannungsversorgung an.

Hinweis Das Beispiel zeigt die Klemmenbelegung eines Sicherheitsnetzwerk-Controllers NE1A-SCPU01(-V1).

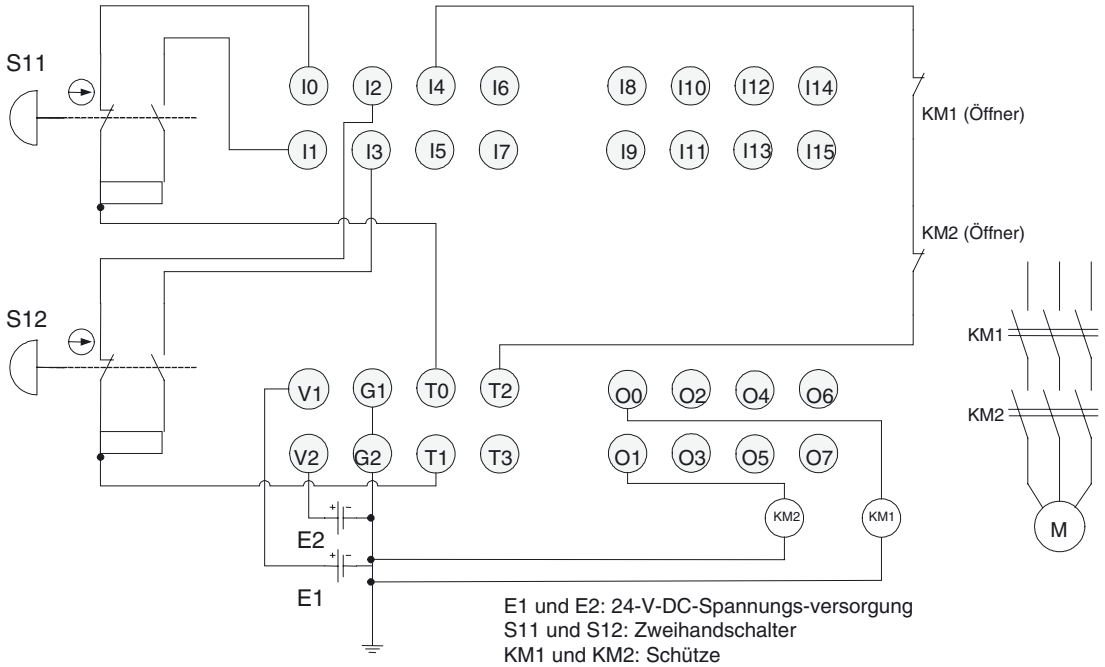
Anschluss eines Positionsschalters (für eine Sicherheitstür)



Hinweis Schließen Sie die Klemmen V0 und G0 (Spannungsversorgung für interne Schaltkreise) an eine 24-V-DC-Spannungsversorgung an.

Hinweis Das Beispiel zeigt die Klemmenbelegung eines Sicherheitsnetzwerk-Controllers NE1A-SCPU01(-V1).

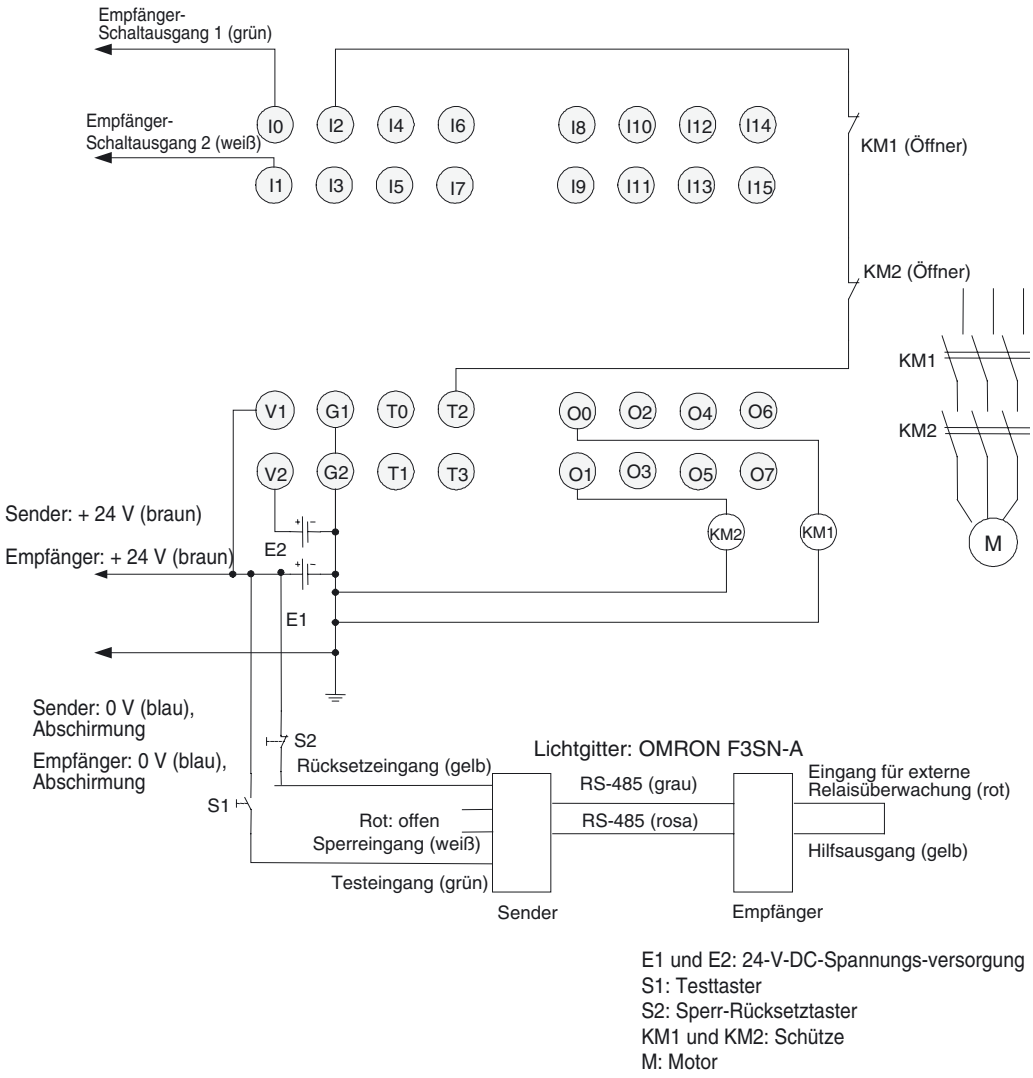
Anschluss eines Zweihandschalters



Hinweis Schließen Sie die Klemmen V0 und G0 (Spannungsversorgung für interne Schaltkreise) an eine 24-V-DC-Spannungsversorgung an.

Hinweis Das Beispiel zeigt die Klemmenbelegung eines Sicherheitsnetzwerk-Controllers NE1A-SCPU01(-V1).

Anschluss eines Lichtgitters

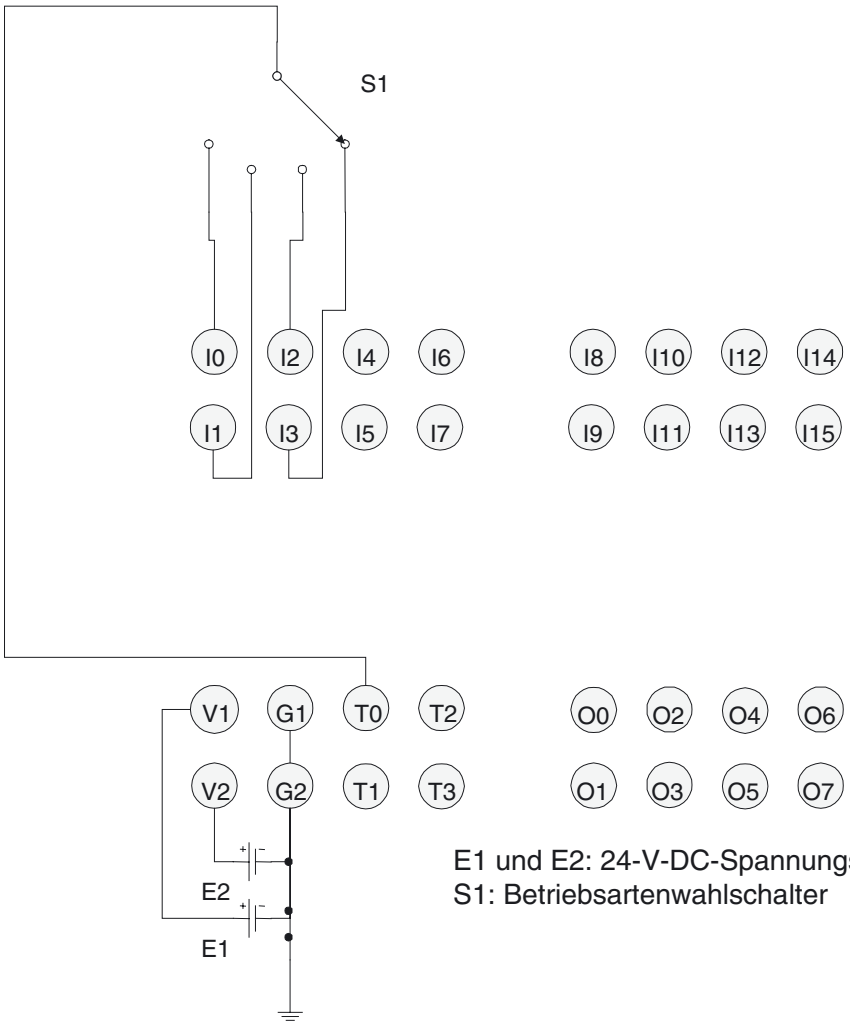


E1 und E2: 24-V-DC-Spannungs-versorgung
S1: Testtaster
S2: Sperr-Rücksetztaster
KM1 und KM2: Schütze
M: Motor

Hinweis Schließen Sie die Klemmen V0 und G0 (Spannungsversorgung für die internen Schaltkreise) an eine 24-V-DC-Spannungsversorgung an.

Hinweis Das Beispiel zeigt die Klemmenbelegung eines Sicherheitsnetzwerk-Controllers NE1A-SCPU01(-V1).

Anschluss eines Betriebsartenwahlschalters



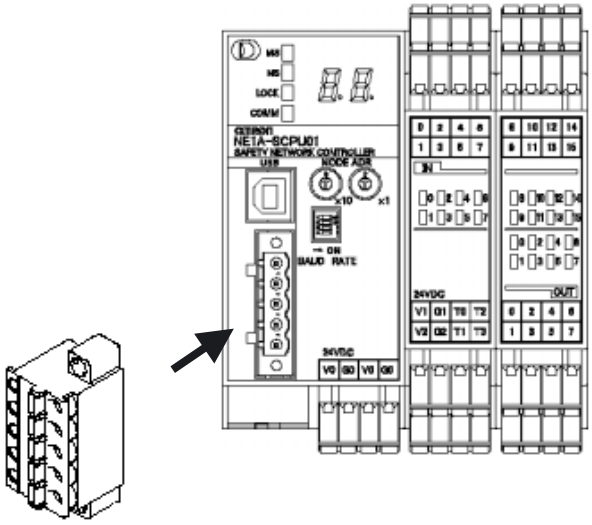
E1 und E2: 24-V-DC-Spannungs-ve
S1: Betriebsartenwahlschalter

Hinweis Schließen Sie die Klemmen V0 und G0 (Spannungsversorgung für interne Schaltkreise) an eine 24-V-DC-Spannungsversorgung an.

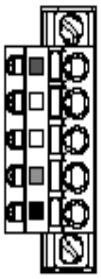
Hinweis Das Beispiel zeigt die Klemmenbelegung eines Sicherheitsnetzwerk-Controllers NE1A-SCPU01(-V1).

3-2-4 DeviceNet-Verdrahtung

Der Anschluss der DeviceNet-Kommunikationskabels erfolgt wie in der nachstehenden Abbildung dargestellt.



Die Kontakte des DeviceNet-Steckers tragen eine Farbkodierung, die der des DeviceNet-Kommunikationskabels entspricht. Achten Sie beim Anschluss des Kabels an den Stecker auf die Übereinstimmung zwischen Kontaktfarbe und Adernfarbe:



Farbe	Beschreibung
Rot	V+
Weiß	Signal (CAN H)
-	Drain
Blau	Signal (CAN L)
Schwarz	V–

WICHTIG

- Schalten Sie vor Beginn der Arbeiten für die DeviceNet-Verdrahtung die Spannungsversorgung des Sicherheitsnetzwerk-Controllers NE1A und aller Netzwerkteilnehmer und Kommunikationsleitungen aus.
- Ziehen Sie den DeviceNet-Stecker mit dem vorgesehenen Drehmoment (0,25 bis 0,3 Nm) fest.
- Halten Sie Leitungen für DeviceNet-Kommunikation getrennt von Strom- oder Hochspannungsleitungen.

Hinweis Weitere Informationen zur Verdrahtung finden Sie im *DeviceNet-Bedienerhandbuch* (Cat. No. W267).

3-2-5 Verdrahtung des USB-Anschlusses

Zur Nutzung des Netzwerkkonfigurators muss der Sicherheitsnetzwerk-Controller NE1A-SCPU01 an einen Standard-PC angeschlossen werden. Verwenden Sie für die USB-Verbindung ein handelsübliches USB-A zu USB-B-Kabel (männlich/männlich).

Hinweis Die Kabellänge darf max. 3 m betragen.

ABSCHNITT 4
DeviceNet-Kommunikationsfunktionen

4-1 Anfangskonfiguration 52
4-1-1 Hardware-Einrichtung 52
4-1-2 Softwareeinstellungen 54
4-2 Netzwerkstatusanzeige 55
4-3 Zuordnung dezentraler E/A-Punke 57
4-3-1 Überblick über die Zuordnung dezentraler E/A-Punke 57
4-3-2 Attribute dezentraler E/A-Bereiche 58
4-3-3 Konfiguration der Daten des dezentralen E/A-Bereichs 59
4-4 Sicherheits-Master-Funktion 69
4-4-1 Sicherheits-E/A-Kommunikation bei Verwendung des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 als Sicherheits-Master 69
4-4-2 Einstellungen für Sicherheits-E/A-Verbindungen 70
4-4-3 Parameter „Connection Type“ 71
4-4-4 Anhalten/Zurücksetzen der Kommunikation nach einem Fehler 72
4-5 Sicherheits-Slave-Funktion 75
4-5-1 Sicherheits-E/A-Kommunikation bei Verwendung des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 als Sicherheits-Slave 75
4-5-2 Erstellung der E/A-Daten (Sicherheits-Slave-E/A) für die Verwendung als Sicherheits-Slave 76
4-6 Standard-Slave-Funktion 79
4-6-1 Sicherheits-E/A-Kommunikation bei Verwendung des Sicherheitsnetzwerk-Controllers NE1A als Standard-Slave 79
4-6-2 Erstellung der E/A-Daten (Slave-E/A) für die Verwendung als Standard-Slave . . 80
4-7 Explicit Message-Kommunikation 83
4-7-1 Empfangen von Explicit Messages 83
4-7-2 Explicit-Message-Übertragung 86

4-1 Anfangskonfiguration

4-1-1 Hardware-Einrichtung

Knotenadresseneinstellung

Die Einstellung der Knotenadresse erfolgt mithilfe der Drehschalter an der Front des Sicherheitsnetzwerk-Controllers NE1A.

Einstellverfahren	Zweistellige Dezimalzahl
Bereich	0 bis 63

Hinweis Ab Werk ist die Knotenadresse auf 63 eingestellt.

Die Knotenadresse kann auf einen beliebigen Wert innerhalb des zulässigen Bereichs eingestellt werden, sofern diese Adresse nicht von einem anderen Knoten verwendet wird. Wenn die Drehschalter auf einen Wert zwischen 64 und 99 eingestellt sind, kann die Einstellung der Knotenadresse durch eine Softwareeinstellung des Netzwerkkonfigurators erfolgen.

Softwareeinstellung

Stellen Sie die Knotenadresse wie folgt mit dem Netzwerkkonfigurator ein:

1. Schalten Sie die Spannungsversorgung aus, und stellen Sie die Drehschalter auf eine Zahl zwischen 64 und 99 (Softwareeinstellung).
2. Schalten Sie die Spannungsversorgung wieder ein. Der Sicherheitsnetzwerk-Controller NE1A arbeitet mit der vorigen Knotenadresse (Werkseinstellung 63).
3. Stellen Sie mit dem Befehl RESET des Netzwerkkonfigurators die Standardeinstellungen wieder her.
   Darauf hin werden die im Gerät enthaltenen Konfigurationsdaten initialisiert.
4. Richten Sie die Knotenadresse über den Netzwerkkonfigurator ein.

Darauf hin arbeitet der Sicherheitsnetzwerk-Controller NE1A mit der Knotenadresse, die über die Software eingerichtet wurde.

WICHTIG

- Schalten Sie vor dem Einrichten der Knotenadresse die Versorgungsspannung des Sicherheitsnetzwerk-Controllers NE1A aus.
- Bei eingeschalteter Spannungsversorgung darf die Einstellung der Drehschalter nicht geändert werden. Erfolgt eine Änderung der Einstellungen bei eingeschalteter Spannungsversorgung, erkennt der Sicherheitsnetzwerk-Controller NE1A dies als Konfigurationsänderung und geht in den Sperr-Zustand über.
- Wurde für mehrere Knoten dieselbe Knotenadresse eingestellt, tritt ein Knotenadressen-Mehrfachverwendungs-Fehler auf. In diesem Fall findet keine Kommunikation im Netzwerk statt.

Hinweis Verwenden Sie zum Einstellen der Drehschalter einen kleinen Schlitzschraubendreher. Achten Sie darauf, die Drehschalter nicht zu beschädigen.

Baudrateneinstellung

Die Einstellung der DeviceNet-Baudrate erfolgt mithilfe der DIP-Schalter an der Front des Sicherheitsnetzwerk-Controllers NE1A. Die folgende Tabelle zeigt die Schaltereinstellungen für die möglichen Baudraten.

DIP-Schalter				Baudrate
1	2	3	4	
OFF	AUS	AUS	AUS	125 kBit/s
EIN	AUS	AUS	AUS	250 kBit/s
AUS	EIN	AUS	AUS	500 kBit/s
EIN	EIN	AUS	AUS	Softwareeinstellung
ON oder OFF	ON oder OFF	EIN	AUS	
ON oder OFF	ON oder OFF	ON oder OFF	EIN	Automatische Erkennung der Baudrate

Hinweis Ab Werk ist die Baudrate auf 125 kBit/s eingestellt.

Softwareeinstellung

Die Einstellung der Baudrate kann auch mithilfe des Netzwerkkonfigurators erfolgen. Dazu bedarf es der folgenden Vorgehensweise:

1. Schalten Sie die Spannungsversorgung aus, und stellen Sie die DIP-Schalter auf „Softwareeinstellung“.
2. Schalten Sie die Spannungsversorgung wieder ein. Nach dem Einschalten der Spannungsversorgung arbeitet der Sicherheitsnetzwerk-Controller NE1A mit der vorigen Baudrate (Standardeinstellung: 125 kBit/s).
3. Stellen Sie mit dem Befehl RESET des Netzwerkkonfigurators die Standardeinstellungen wieder her.
   Darauf hin werden die im Gerät enthaltenen Konfigurationsdaten initialisiert.
4. Stellen Sie mithilfe des Netzwerkkonfigurators die Baudrate ein.
5. Führen Sie einen Neustart des Sicherheitsnetzwerk-Controllers NE1A durch (Aus- und Einschalten der Spannungsversorgung oder Ausführung des NE1A-Befehls RESET vom Netzwerkkonfigurator aus). Anschließend kommuniziert der Sicherheitsnetzwerk-Controller NE1A mit der durch den Netzwerkkonfigurator eingestellten Baudrate, d. h. der Softwareeinstellung.

Automatische Erkennung der Baudrate

Die Baudrate des Sicherheitsnetzwerk-Controllers NE1A kann automatisch auf die Baudrate des Netzwerk-Masters eingestellt werden. Dazu muss bei mindestens einem Sicherheits- oder Standard-Master im Netzwerk die Einstellung der Baudrate erfolgt sein. Diese Baudrate wird nach dem Einschalten der Spannungsversorgung und der Aufnahme der Kommunikation automatisch übernommen und bleibt bis zum Ausschalten der Spannungsversorgung gespeichert.

WICHTIG

- Schalten Sie vor dem Verstellen des DIP-Schalters die Versorgungsspannung des Sicherheitsnetzwerk-Controllers NE1A aus.
- Die Einstellungen der DIP-Schalter dürfen nur bei ausgeschalteter Spannungsversorgung geändert werden. Erfolgt eine Änderung der Einstellungen bei eingeschalteter Spannungsversorgung, erkennt der Sicherheitsnetzwerk-Controller NE1A dies als Konfigurationsänderung und geht in den Sperr-Zustand über.
- Die Baudrateneinstellung aller Knoten im Netzwerk (Master und Slaves) muss identisch sein.

4-1-2 Softwareeinstellungen

Einstellung „DeviceNet-Kommunikation deaktiviert (Standalone)“

Ist die DeviceNet-Kommunikation deaktiviert, stellt der Sicherheitsnetzwerk-Controller NE1A jegliche DeviceNet-Kommunikation ein und fungiert als Standalone-Controller. Standardmäßig ist die DeviceNet-Kommunikation aktiviert (normaler Modus).

Diese Einstellung erfolgt mithilfe des Netzwerkkonfigurators. Nach Änderung dieser Einstellung sendet der Netzwerkkonfigurator einen Rücksetzbefehl an den Sicherheitsnetzwerk-Controller NE1A, um die geänderte Einstellung zu aktivieren.

Einstellung	Beschreibung
Aktiviert (normaler Modus)	DeviceNet-Kommunikation aktiviert.
Deaktiviert (Standalone-Controller-Modus)	DeviceNet-Kommunikation deaktiviert. Der Sicherheitsnetzwerk-Controller NE1A-SCPU01 fungiert als Standalone-Controller. Die Siebensegmentanzeige zeigt „nd“ an.

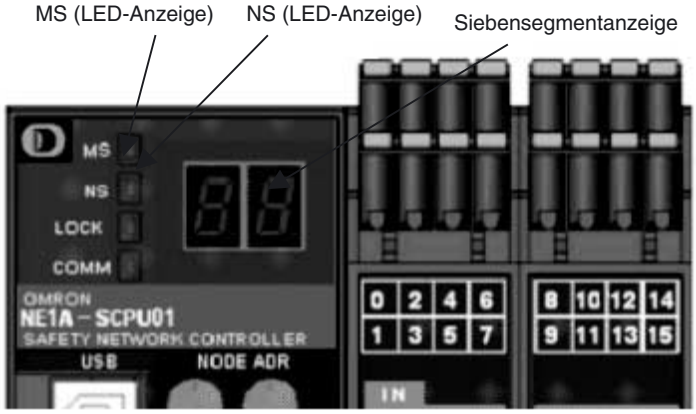
WICHTIG

- Ist die DeviceNet-Kommunikation deaktiviert, muss der Sicherheitsnetzwerk-Controller NE1A über eine USB-Verbindung an den Netzwerkkonfigurator angeschlossen werden.
- Ist die DeviceNet-Kommunikation deaktiviert, ist der Betrieb des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 nur über eine USB-Verbindung mit dem Netzwerkkonfigurator möglich.

4-2 Netzwerkstatusanzeige

Die LED-Anzeige „NS“ (Netzwerkstatus) gibt Aufschluss über den Netzwerkstatus des Sicherheitsnetzwerk-Controllers NE1A.

Im normalen Betrieb zeigt die Siebensegmentanzeige die Knotenadresse des Sicherheitsnetzwerk-Controller NE1A. Im Fehlerfall zeigt sie abwechselnd den Fehlercode und die Knotenadresse des Geräts, bei dem der Fehler auftrat. Ist die DeviceNet-Kommunikation deaktiviert (Standalone-Controller-Modus), zeigt die Siebensegmentanzeige im normalen Betrieb „nd“.



LED-Anzeigen „MS“ und „NS“

Bezeichnung der LED-Anzeige	Farbe	Status	Bedeutung
MS (Baugruppenstatus)	Grün	☐	Normalbetrieb
		◪	Leerlauf
	Rot	☐	Kritischer Fehler
		◪	Abbruch
	Grün/Rot	◪	Warten auf TUNID-Einstellung während der Selbstdiagnose oder Warten auf Konfiguration
	-	■	Spannungsversorgung ausgeschaltet
NS (Netzwerkstatus)	Grün	☐	Online-Verbindung besteht
		◪	Online-Verbindung besteht nicht
	Rot	☐	Kommunikation nicht möglich
		◪	E/A-Kommunikationsfehler
	Grün/Rot	◪	Warten auf TUNID-Einstellung
	-	■	Nicht online (inkl. Standalone-Controller-Modus)

☐ : Leuchtet ◪ : Blinkt ■ : AUS

Siebensegmentanzeige

Im normalen Betrieb zeigt die Siebensegmentanzeige die Knotenadresse des Sicherheitsnetzwerk-Controller NE1A. Im Fehlerfall zeigt sie abwechselnd den Fehlercode und die Knotenadresse des Geräts, bei dem der Fehler auftrat. Ist die DeviceNet-Kommunikation deaktiviert (Standalone-Controller-Modus), zeigt die Siebensegmentanzeige im normalen Betrieb „nd“.

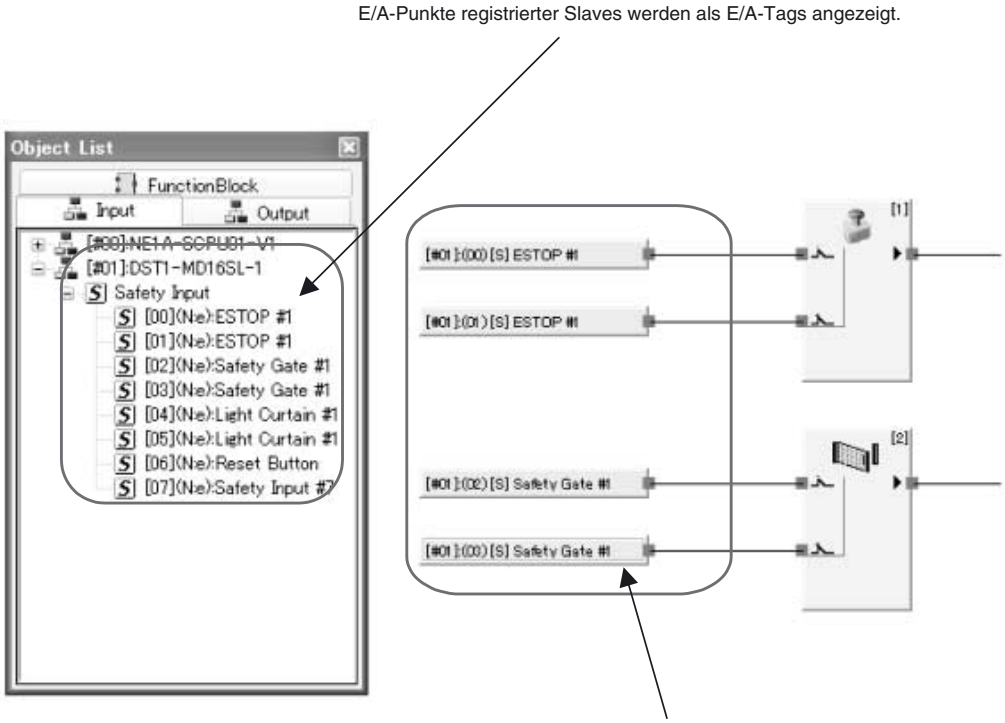
Status		Anzeige	
Normaler Betrieb, DeviceNet-Kommunikation aktiviert	Betriebsmodus: RUN Sicherheits-E/A-Kommunikation: in Betrieb oder nicht eingerichtet	Knotenadresse des Sicherheitsnetzwerk-Controllers (00 bis 63)	Leuchtet
	Betriebsmodus: RUN Sicherheits-E/A-Kommunikation: Nicht in Betrieb		Blinkt
	Betriebsmodus: Selbsttest, konfigurierend oder Leerlauf		Blinkt
Normaler Betrieb, DeviceNet-Kommunikation deaktiviert	Betriebsmodus: RUN	„nd“	Leuchtet
	Betriebsmodus: Selbsttest, konfigurierend oder Leerlauf		Blinkt
Fehlerzustände	Kritischer Fehler	Unbestimmt	
		Nur Fehlercode	Leuchtet
	Abbruch	Nur Fehlercode	Leuchtet
	Geringfügiger Fehler	Abwechselnd Fehlercode und die Knotenadresse des Geräts, bei dem der Fehler auftrat	

Hinweis Die Anzeige von Fehlern erfolgt durch entsprechende Kombinationen der LED-Anzeigen „MS“ und „NS“ und der Siebensegmentanzeige. Detailinformationen zur Bedeutung dieser Kombinationen finden Sie in *Kapitel 10: Fehlersuche.*

4-3 Zuordnung dezentraler E/A-Punke

4-3-1 Überblick über die Zuordnung dezentraler E/A-Punke

Die von dezentralen Sicherheits-Mastern und -Slaves sowie Standard-Mastern und -Slaves bereitgestellten E/A-Bereiche werden gemäß der mit dem Netzwerkkonfigurator vorgenommenen Einstellungen automatisch im E/A-Speicher des Sicherheitsnetzwerk-Controllers NE1A zugeordnet. Die Anzeige der E/A-Punkte im Netzwerk erfolgt als E/A-Tags. Diese ermöglichen die Programmierung ohne Kenntnis der exakten Speicheradressen im Sicherheitsnetzwerk-Controller NE1A.



4-3-2 Attribute dezentraler E/A-Bereiche

Attribute dezentraler E/A-Bereiche

Der dezentrale E/A-Bereich des Sicherheitsnetzwerk-Controllers NE1A besitzt die folgenden Attribute.

Bei einer Änderung des Betriebsmodus werden alle Werte im E/A-Bereich einer dezentralen Sicherheitsbaugruppe gelöscht. Beim Auftreten eines Kommunikationsfehlers werden alle von der fehlerhaften Verbindung betroffenen Daten gelöscht.

	Änderung des Betriebsmodus		**Kommunikatinsfehler**	**Einschalten der Spannungsversorgung**
	RUN to Idle	**RUN oder IDLE CONFIGURING**		
E/A-Bereich der dezentralen Sicherheitsbaugruppe (DeviceNet Safety)	Gelöscht (Sicherheitszustand)	Gelöscht (Sicherheitszustand)	Gelöscht für die fehlerhafte Verbindung (Sicherheitszustand)	Gelöscht (Sicherheitszustand)
Dezentraler E/A-Standardbereich (DeviceNet)	Abhängig von der Halteeinstellung für den E/A-Bereich des Slaves	Gelöscht	Abhängig von der Halteeinstellung für den E/A-Bereich des Slaves	Gelöscht

Hinweis Detaillierte Informationen zu den Betriebsmodi finden Sie im *Abschnitt 8 Betriebsmodi und Unterbrechungen der Spannungsversorgung*.

Speichereinstellung für den E/A-Bereich von Slaves

Einstellung	**Beschreibung**	**Standardeinstellung**	**Gültigkeit**
Löschen	Beim Auftreten eines Kommunikationsfehlers in der Verbindung wird der Ausgangsbereich der Slaves (Eingänge für das Anwenderprogramm) gelöscht. Bei einem Wechsel des Betriebsmodus nach „IDLE“ wird der Eingangsbereich der Slaves (Ausgänge des Masters) gelöscht.	Löschen	Beim Aus- und Wiedereinschalten
Speichern	Beim Auftreten eines Kommunikationsfehlers in der Verbindung werden die letzten Daten des Ausgangsbereichs der Slaves (Eingänge für das Anwenderprogramm) gespeichert. Bei einem Wechsel des Betriebsmodus nach „IDLE“ werden die letzten Daten des Eingangsbereichs der Slaves (Ausgänge des Masters) gelöscht. Beim Auftreten eines kritischen Fehlers, bei einem Abbruch oder beim Wiedereinschalten der Spannungsversorgung werden die Werte jedoch gelöscht.		

4-3-3 Konfiguration der Daten des dezentralen E/A-Bereichs

Mit dem Netzwerkkonfigurator können die Daten spezifiziert werden, die vom Sicherheitsnetzwerk-Controller NE1A als Sicherheits-Slave oder Standard-Slave-Eingangsdaten übertragen wurden. Dieser Abschnitt beschreibt die einstellbaren Daten, die Einstellmethode und die Datenkonfiguration.

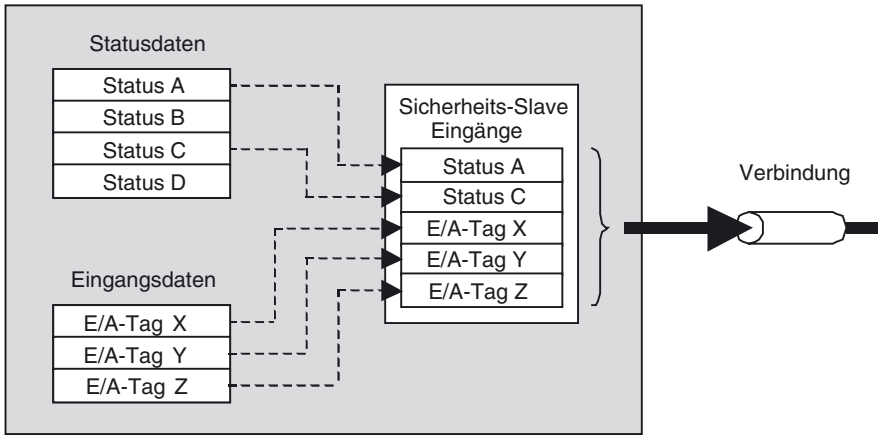
Konfiguration von zu übertragenden Daten

Die Sicherheitsnetzwerk-Controller NE1A vor Version 1.0 können Statusdaten und E/A-Daten kombinieren und als dezentrale E/A-Daten übertragen.

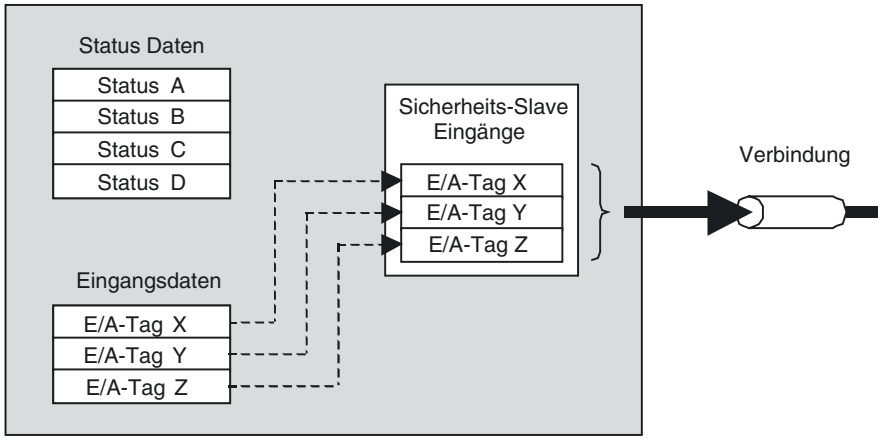
Sicherheitsnetzwerk-Controller NE1A ab Version 1.0 können Statusdaten, lokale E/A-Überwachungsdaten und E/A-Daten kombinieren und als dezentrale E/A-Daten übertragen.

Welche Daten übertragen werden, wird über die Konfiguration bestimmt. Die Daten werden normalerweise in der Reihenfolge Statusdaten, lokale E/A-Überwachungsdaten und E/A-Daten konfiguriert. Die Statusdaten können in der SPS gesammelt werden, um ein Überwachungssystem zu erzeugen. Es können auch ausschließlich Statusdaten oder nur lokale E/A-Überwachungsdaten oder nur E/A-Daten konfiguriert werden.

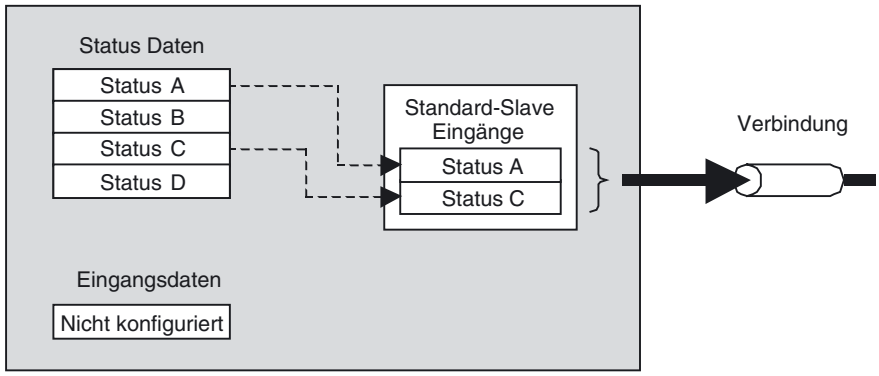
Beispiel 1: Übertragung von Statusdaten und E/A-Tags als Sicherheits-Slave-Eingänge



Beispiel 2: Übertragung von ausschließlich E/A-Tags als Sicherheits-Slave-Eingänge



Beispiel 3: Übertragung von ausschließlich Statusdaten als Standard-Slave-Eingänge



Einstellbare Daten und Anordnungsbeispiele

Die nachstehende Tabelle zeigt die einstellbaren Daten.

• Sicherheitsnetzwerk-Controllers NE1A vor Version 1.0

Datentyp	Bezeichnung/Format	Daten-größe	Einstellmethode mit Netzwerkkonfigurator	Attribut
Status	Allgemeiner Status	Byte	Einstellung über Kontroll-kästchen	nicht sicher
	Status der lokalen Eingänge	Wort	Einstellung über Kontroll-kästchen	Safety
	Status der lokalen Ausgänge	Byte	Einstellung über Kontroll-kästchen	Safety
	Status der Testausgänge/Muting-Lampe	Byte	Einstellung über Kontroll-kästchen	nicht sicher
E/A-Tags	BOOL E/A-Tags	Byte	Benutzerregistriert	Safety
	BYTE E/A-Tags	Byte	Benutzerregistriert	Safety
	WORD E/A-Tags	Wort	Benutzerregistriert	Safety
	DWORD (Doppelwort) E/A-Tags	Doppel-wort	Benutzerregistriert	Safety

• Sicherheitsnetzwerk-Controller NE1A ab Version 1.0

Datentyp	Bezeichnung/Format	Daten-größe	Einstellmethode mit Netzwerkkonfigurator	Attribut
Status	Allgemeiner Status	Byte	Einstellung über Kontroll-kästchen	nicht sicher
	Lokaler E/A-Status 1 bis N (siehe Hinweis 1.)	Byte	Einstellung über Kontroll-kästchen	Safety
	Status der lokalen Ausgänge	Byte	Einstellung über Kontroll-kästchen	Safety
	Status der Testausgänge/Muting-Lampe 1 bis M (siehe Hinweis 1.)	Byte	Einstellung über Kontroll-kästchen	nicht sicher
Lokale E/A-Überwa-chung	Lokale Eingangsüberwachung 1 bis N (siehe Hinweis 1.)	Byte	Einstellung über Kontroll-kästchen	Safety
	Lokale Ausgangsüberwachung	Byte	Einstellung über Kontroll-kästchen	Safety
E/A-Tags	BOOL E/A-Tags	Byte	Benutzerregistriert	Safety
	BYTE E/A-Tags	Byte	Benutzerregistriert	Safety
	WORD E/A-Tags	Wort	Benutzerregistriert	Safety
	DWORD (Doppelwort) E/A-Tags	Doppel-wort	Benutzerregistriert	Safety

Hhweis

(1) Bei NE1A-SCPU01-V1 N = 2 und M = 1. Bei NE1A-SCPU02 N = 5 und M = 2. Die Datengröße für lokalen Eingangsstatus, Testausgang-/Mutingleuchtenstatus und lokalen Eingangsüberwachungsstatus kann in Byte angegeben werden.

(2) Die erforderlichen Maßnahmen zur Handhabung von Daten als Sicherheitsdaten bei der Datenerstellung werden nicht für Status- und E/A-Tag-Daten mit dem Attribut „nicht sicher“ ergriffen. Diese Positionen dürfen daher nicht für die Konfiguration eines Sicherheitssystems verwendet werden.
Selbst wenn das Attribut für ein Element „sicher“ lautet, wird es zu „nicht sicher“ bei Dateneingaben über Standard-E/A-Kommunikation sowie bei E/A-Tags, die mit Standardbaugruppen verbunden sind. Auch diese Elemente dürfen daher nicht für die Konfiguration eines Sicherheitssystems verwendet werden.

Wenn die obigen Daten kombiniert sind, werden die E/A-Daten wie folgt konfiguriert:

1. Wenn Statusdaten gesetzt sind, wird der Status am Anfang des dezentralen E/A-Bereichs in der unten gezeigten Reihenfolge zugewiesen. (Nicht gesetzte Statusbereiche werden nicht freigehalten, d.h. es bleiben keine Bereiche ohne Zuweisung übrig.)

   Allgemeiner Status
   ↓
   Status der lokalen Eingänge
   ↓
   Status der lokalen Ausgänge
   ↓
   Status der Testausgänge/Muting-Lampe

2. Wenn die lokalen E/A-Überwachungsdaten gesetzt sind (Controller ab Geräteversion 1.0), werden die lokalen E/A-Überwachungsdaten in der folgenden Reihenfolge hinter den übrigen Statusdaten angehängt. (Wenn keine lokalen E/A-Überwachungsdaten gesetzt sind, werden die Daten nach vorn gerückt, und der entsprechende lokale E/A-Überwachungsbereich wird nicht freigehalten. Dieser Bereich existiert nicht bei Controllern vor Version 1.0)

   Lokale Eingangsüberwachung
   ↓
   Lokale Ausgangsüberwachung

3. Nach den Statusdaten und den lokalen E/A-Überwachungsdaten werden dem dezentralen E/A-Bereich benutzerregistrierte E/A-Tags in der Reihenfolge der Registrierung zugewiesen. Zu diesem Zeitpunkt werden keine freien Bereiche freigehalten, und alle gültigen Daten werden ohne zuweisungsfreie Bereiche zugewiesen.

Weiter unten finden Sie einige Beispiele für Einstellungen mittels Netzwerkkonfigurator nebst Anordnung des dezentralen Bereichs.

Einstellungsbeispiel 1: Einstellung mittels Netzwerkkonfigurator (ab Geräteversion 1.0)

Die nachstehende Tabelle verdeutlicht die Anordnung des dezentralen E/A-Bereichs, wenn die obigen Einstellungen vorgenommen werden.

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Allgemeiner Status (1 Byte)							
1	Lokaler Eingangsstatus 1 (1 Byte)							
2	Lokaler Eingangsstatus 2 (1 Byte)							
3	Lokaler Ausgangsstatus (1 Byte)							
4	Status der Testausgänge/Muting-Lampe (1 Byte)							
5	Byte A (1 Byte)							
6	Wort B (2 Bytes)							
7								

Einstellungsbeispiel 2: Einstellung mittels Netzwerkkonfigurator (ab Geräteversion 1.0)

Die nachstehende Tabelle verdeutlicht die Anordnung des dezentralen E/A-Bereichs, wenn die obigen Einstellungen vorgenommen werden.

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Lokaler Eingangsstatus 1 (1 Byte)							
1	Lokaler Eingangsstatus 2 (1 Byte)							
2	Lokaler Ausgangsstatus (1 Byte)							
3	Bool C (1 Byte)							
4	Dword D (4 Bytes)							
5								
6								
7								

Einstellungsbeispiel 3: Einstellung mittels Netzwerkkonfigurator (Controller ab Geräteversion 1.0)

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Lokaler Eingangsstatus 1 (1 Byte)							
1	Lokaler Eingangsstatus 3 (1 Byte)							
2	Lokaler Eingangsstatus 5 (1 Byte)							
3	Lokaler Ausgangsstatus (1 Byte)							
4	Lokale Eingangsüberwachung 1 (1 Byte)							
5	Lokale Eingangsüberwachung 3 (1 Byte)							
6	Lokale Eingangsüberwachung 5 (1 Byte)							
7	Lokale Ausgangsüberwachung (1 Byte)							
8	Bool E (1 Byte)							
9	Byte F (1 Byte)							

Bit-Anordnung für den jeweiligen Datentyp

Nachstehend sind die Bit-Anordnungen für Statusdaten- und E/A-Tag-Einstellungen aufgeführt.

Statusdetails

Die nachstehenden Tabellen verdeutlichen die Statusdetails.

Allgemeiner Status (1 Byte) Attribut: nicht sichere Daten

Bit	Inhalt	Beschreibung
0	Statusmerker für die Versorgungsspannung der Eingänge AUS: Die normale Versorgungsspannung ist eingeschaltet. EIN: Fehler in der Versorgungsspannung oder Versorgungsspannung ist ausgeschaltet.	Status der Versorgungsspannung der Eingänge.
1	Statusmerker für die Versorgungsspannung der Ausgänge AUS: Die normale Versorgungsspannung ist eingeschaltet. EIN: Fehler in der Versorgungsspannung oder Versorgungsspannung ist ausgeschaltet.	Status der Versorgungsspannung der Ausgänge.
2	Fehlermerker für die Standard-E/A-Kommunikation AUS: Kein Fehler EIN: Fehler	Dieser Merker gibt an, ob ein Fehler in der Standard-E/A-Kommunikation vorliegt. Die Angabe „Fehler“ kann sich auf eine oder mehrere Verbindungen beziehen.
3	Statusmerker für die Standard-E/A-Kommunikation AUS: E/A-Kommunikation angehalten oder Fehler EIN: E/A-Kommunikation wird durchgeführt	Dieser Statusmerker gibt an, ob Standard-E/A-Kommunikation durchgeführt wird. Die Angabe „EIN“ gibt an, dass über alle Verbindungen normale Kommunikation durchgeführt wird.
4	Fehlermerker für die Sicherheits-E/A-Kommunikation AUS: Kein Fehler EIN: Fehler	Dieser Merker gibt an, ob ein Fehler in der Sicherheits-E/A-Kommunikation vorliegt. Die Angabe „Fehler“ kann sich auf eine oder mehrere Verbindungen beziehen.
5	Statusmerker für die Sicherheits-E/A-Kommunikation AUS: E/A-Kommunikation angehalten oder Fehler EIN: E/A-Kommunikation wird durchgeführt	Dieser Statusmerker gibt an, ob Sicherheits-E/A-Kommunikation durchgeführt wird. Die Angabe „EIN“ gibt an, dass über alle Verbindungen normale Kommunikation durchgeführt wird.
6	Betriebsmodus-Merker AUS: Anderer Betriebsmodus als „RUN“ EIN: RUN (Betrieb)	Aktueller Betriebsmodus des Sicherheitsnetzwerk-Controllers NE1A.
7	NE1A-Status-Merker AUS: Fehler EIN: Normal	Aktueller Status des Sicherheitsnetzwerk-Controllers NE1A Dieser Merker zeigt einen Fehler an, wenn ein Fehler in den Fehlerdetails (*10-4-2 Fehlerinformationen im Detail*) auftritt.

Status des lokalen Eingangs(2 Bytes, Controller vor Version 1.0)Attribut: sichere Daten

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Klemmenstatus Sicherheitseingang 7	Klemmenstatus Sicherheitseingang 6	Klemmenstatus Sicherheitseingang 5	Klemmenstatus Sicherheitseingang 4	Klemmenstatus Sicherheitseingang 3	Klemmenstatus Sicherheitseingang 2	Klemmenstatus Sicherheitseingang 1	Klemmenstatus Sicherheitseingang 0
1	Klemmenstatus Sicherheitseingang 15	Klemmenstatus Sicherheitseingang 14	Klemmenstatus Sicherheitseingang 13	Klemmenstatus Sicherheitseingang 12	Klemmenstatus Sicherheitseingang 11	Klemmenstatus Sicherheitseingang 10	Klemmenstatus Sicherheitseingang 9	Klemmenstatus Sicherheitseingang 8

EIN: Normal / AUS: Fehler

Lokaler Eingangstatus 1 (1 Byte, Controller ab Version 1.0)Attribut: sichere Daten

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Klemmen-status Sicherheits-eingang 7	Klemmen-status Sicherheits-eingang 6	Klemmen-status Sicherheits-eingang 5	Klemmen-status Sicherheits-eingang 4	Klemmen-status Sicherheits-eingang 3	Klemmen-status Sicherheits-eingang 2	Klemmen-status Sicherheits-eingang 1	Klemmen-status Sicherheits-eingang 0

EIN: Normal / AUS: Fehler

Lokaler Eingangstatus 2 (1 Byte, Controller ab Version 1.0)Attribut: sichere Daten

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Klemmen-status Sicherheit-eingang 15	Klemmen-status Sicherheit-eingang 14	Klemmen-status Sicherheit-eingang 13	Klemmen-status Sicherheit-eingang 12	Klemmen-status Sicherheit-eingang 11	Klemmen-status Sicherheit-eingang 10	Klemmen-status Sicherheit-eingang 9	Klemmen-status Sicherheit-eingang 8

EIN: Normal / AUS: Fehler

Lokaler Eingangsstatus 3 (1 Byte, NE1A-SCPU02) Attribut: sichere Daten

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Klemmen-status Sicherheit-eingang 23	Klemmen-status Sicherheit-eingang 22	Klemmen-status Sicherheit-eingang 21	Klemmen-status Sicherheit-eingang 20	Klemmen-status Sicherheit-eingang 19	Klemmen-status Sicherheit-eingang 18	Klemmen-status Sicherheit-eingang 17	Klemmen-status Sicherheit-eingang 16

EIN: Normal / AUS: Fehler

Lokaler Eingangsstatus 4 (1 Byte, NE1A-SCPU02) Attribut: sichere Daten

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Klemmen-status Sicherheit-eingang 31	Klemmen-status Sicherheit-eingang 30	Klemmen-status Sicherheit-eingang 29	Klemmen-status Sicherheit-eingang 28	Klemmen-status Sicherheit-eingang 27	Klemmen-status Sicherheit-eingang 26	Klemmen-status Sicherheit-eingang 25	Klemmen-status Sicherheit-eingang 24

EIN: Normal / AUS: Fehler

Lokaler Eingangsstatus 5 (1 Byte, NE1A-SCPU02) Attribut: sichere Daten

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Klemmen-status Sicherheit-eingang 39	Klemmen-status Sicherheit-eingang 38	Klemmen-status Sicherheit-eingang 37	Klemmen-status Sicherheit-eingang 36	Klemmen-status Sicherheit-eingang 35	Klemmen-status Sicherheit-eingang 34	Klemmen-status Sicherheit-eingang 33	Klemmen-status Sicherheit-eingang 32

EIN: Normal / AUS: Fehler

Status der lokalen Ausgänge (1 Byte) Attribut: sichere Daten

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Klemmen-status Sicherheit-eingang 7	Klemmen-status Sicherheit-eingang 6	Klemmen-status Sicherheit-eingang 5	Klemmen-status Sicherheit-eingang 4	Klemmen-status Sicherheit-eingang 3	Klemmen-status Sicherheit-eingang 2	Klemmen-status Sicherheit-eingang 1	Klemmen-status Sicherheit-eingang 0

EIN: Normal / AUS: Fehler

Status der Testausgänge/Muting-Lampe (1 Byte) (vor Version 1.0) Attribut: nicht sicher

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Unterbrechung an Testausgangsklemme 3	Reserviert			Klemmenstatus Testausgang 3	Klemmenstatus Testausgang 2	Klemmenstatus Testausgang 1	Klemmenstatus Testausgang 0

EIN: Normal / AUS: Fehler

Status der Testausgänge/Muting-Lampe 1 (1 Byte) (ab Version 1.0) Attribut: nicht sicher

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Unterbrechung an Testausgang 3	Reserviert			Unterbrechung an Testausgang 3	Unterbrechung an Testausgang 2	Unterbrechung an Testausgang 1	Unterbrechung an Testausgang 0

EIN: Normal / AUS: Fehler

Status der Testausgänge/Muting-Lampe 2 (NE1A-SCPU02) Attribut: nicht sicher

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Unterbrechung an Testausgang 7	Reserviert			Unterbrechung an Testausgang 7	Unterbrechung an Testausgang 6	Unterbrechung an Testausgang 5	Unterbrechung an Testausgang 4

EIN: Normal / AUS: Fehler

Lokale Eingangsüberwachung 1 (1 Byte, Controller ab Version 1.0) Attribut: sichere Daten

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Überwachung Klemmenstatus Sicherheitseingang 7	Überwachung Klemmenstatus Sicherheitseingang 6	Überwachung Klemmenstatus Sicherheitseingang 5	Überwachung Klemmenstatus Sicherheitseingang 4	Überwachung Klemmenstatus Sicherheitseingang 3	Überwachung Klemmenstatus Sicherheitseingang 2	Überwachung Klemmenstatus Sicherheitseingang 1	Überwachung Klemmenstatus Sicherheitseingang 0

EIN: Normal / AUS: Fehler

Lokale Eingangsüberwachung 2 (1 Byte, Controller ab Version 1.0) Attribut: sichere Daten

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Überwachung Klemmenstatus Sicherheitseingang 15	Überwachung Klemmenstatus Sicherheitseingang 14	Überwachung Klemmenstatus Sicherheitseingang 13	Überwachung Klemmenstatus Sicherheitseingang 12	Überwachung Klemmenstatus Sicherheitseingang 11	Überwachung Klemmenstatus Sicherheitseingang 10	Überwachung Klemmenstatus Sicherheitseingang 9	Überwachung Klemmenstatus Sicherheitseingang 8

EIN: Normal / AUS: Fehler

Lokale Eingangsüberwachung 3 (1 Byte, NE1A-SCPU02) Attribut: sichere Daten

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Überwachung Klemmenstatus Sicherheitseingang 23	Überwachung Klemmenstatus Sicherheitseingang 22	Überwachung Klemmenstatus Sicherheitseingang 21	Überwachung Klemmenstatus Sicherheitseingang 20	Überwachung Klemmenstatus Sicherheitseingang 19	Überwachung Klemmenstatus Sicherheitseingang 18	Überwachung Klemmenstatus Sicherheitseingang 17	Überwachung Klemmenstatus Sicherheitseingang 16

EIN: Normal / AUS: Fehler

Lokale Eingangsüberwachung 4 (1 Byte, NE1A-SCPU02) Attribut: sichere Daten

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Überwachung Klemmenstatus Sicherheitseingang 31	Überwachung Klemmenstatus Sicherheitseingang 30	Überwachung Klemmenstatus Sicherheitseingang 29	Überwachung Klemmenstatus Sicherheitseingang 28	Überwachung Klemmenstatus Sicherheitseingang 27	Überwachung Klemmenstatus Sicherheitseingang 26	Überwachung Klemmenstatus Sicherheitseingang 25	Überwachung Klemmenstatus Sicherheitseingang 24

EIN: Normal / AUS: Fehler

Lokale Eingangsüberwachung 5 (1 Byte, NE1A-SCPU02) Attribut: sichere Daten

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Überwachung Klemmenstatus Sicherheitseingang 39	Überwachung Klemmenstatus Sicherheitseingang 38	Überwachung Klemmenstatus Sicherheitseingang 37	Überwachung Klemmenstatus Sicherheitseingang 36	Überwachung Klemmenstatus Sicherheitseingang 35	Überwachung Klemmenstatus Sicherheitseingang 34	Überwachung Klemmenstatus Sicherheitseingang 33	Überwachung Klemmenstatus Sicherheitseingang 32

EIN: Normal / AUS: Fehler

Überwachung der lokalen Ausgänge (1 Byte) **Attribut: sichere Daten**

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Überwachung Klemmenstatus Sicherheitsausgang 7	Überwachung Klemmenstatus Sicherheitsausgang 6	Überwachung Klemmenstatus Sicherheitsausgang 5	Überwachung Klemmenstatus Sicherheitsausgang 4	Überwachung Klemmenstatus Sicherheitsausgang 3	Überwachung Klemmenstatus Sicherheitsausgang 2	Überwachung Klemmenstatus Sicherheitsausgang 1	Überwachung Klemmenstatus Sicherheitsausgang 0

EIN: Normal / AUS: Fehler

E/A-Tag-Details

Die nachstehenden Tabellen enthalten die E/A-Tag-Details.

BOOL

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Offen (=0)							Benutzer-daten Bit 0

BYTE

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Benutzer-daten Bit 7	Benutzer-daten Bit 6	Benutzer-daten Bit 5	Benutzer-daten Bit 4	Benutzer-daten Bit 3	Benutzer-daten Bit 2	Benutzer-daten Bit 1	Benutzer-daten Bit 0

WORD

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Benutzer-daten Bit 7	Benutzer-daten Bit 6	Benutzer-daten Bit 5	Benutzer-daten Bit 4	Benutzer-daten Bit 3	Benutzer-daten Bit 2	Benutzer-daten Bit 1	Benutzer-daten Bit 0
1	Benutzer-daten Bit 15	Benutzer-daten Bit 14	Benutzer-daten Bit 13	Benutzer-daten Bit 12	Benutzer-daten Bit 11	Benutzer-daten Bit 10	Benutzer-daten Bit 9	Benutzer-daten Bit 8

DWORD

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Benutzer-daten Bit 7	Benutzer-daten Bit 6	Benutzer-daten Bit 5	Benutzer-daten Bit 4	Benutzer-daten Bit 3	Benutzer-daten Bit 2	Benutzer-daten Bit 1	Benutzer-daten Bit 0
1	Benutzer-daten Bit 15	Benutzer-daten Bit 14	Benutzer-daten Bit 13	Benutzer-daten Bit 12	Benutzer-daten Bit 11	Benutzer-daten Bit 10	Benutzer-daten Bit 9	Benutzer-daten Bit 8
2	Benutzer-daten Bit 23	Benutzer-daten Bit 22	Benutzer-daten Bit 21	Benutzer-daten Bit 20	Benutzer-daten Bit 19	Benutzer-daten Bit 18	Benutzer-daten Bit 17	Benutzer-daten Bit 16
3	Benutzer-daten Bit 31	Benutzer-daten Bit 30	Benutzer-daten Bit 29	Benutzer-daten Bit 28	Benutzer-daten Bit 27	Benutzer-daten Bit 26	Benutzer-daten Bit 25	Benutzer-daten Bit 24

Nicht genutzte Bits unter den oben aufgeführten benutzerregistrierten E/A-Tags werden auf 0 festgelegt.

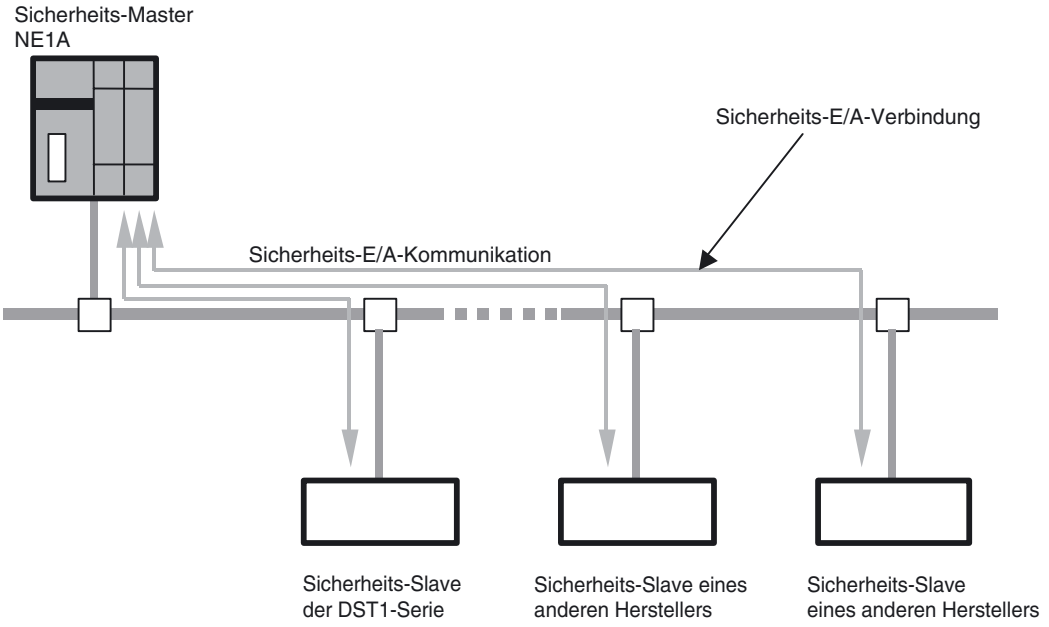
4-4 Sicherheits-Master-Funktion

4-4-1 Sicherheits-E/A-Kommunikation bei Verwendung des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 als Sicherheits-Master

Sicherheits-E/A-Kommunikation ermöglicht den automatischen Datenaustausch mit Sicherheits-Slaves ohne Anwenderprogrammierung.

Die Durchführung einer Sicherheits-E/A-Kommunikation mit anderen Slaves erfordert die folgenden Maßnahmen:

1. Registrierung des Slave-Geräts im Sicherheitsnetzwerk-Controller NE1A.
2. Einrichten der Einstellungen für die Sicherheits-E/A-Verbindung.



Spezifikationen bei Verwendung als Sicherheits-Master

Sicherheits-E/A-Verbindungen	
Anzahl der Verbindungen	Controller vor Version 1.0: max. 16 Controller ab Version 1.0: max. 32
Maximale Datengröße	16 Bytes Eingabedaten oder 16 Bytes Ausgabedaten (je Verbindung)
Verbindungsart	Singlecast oder Multicast

Zuordnung von Sicherheits-Slaves

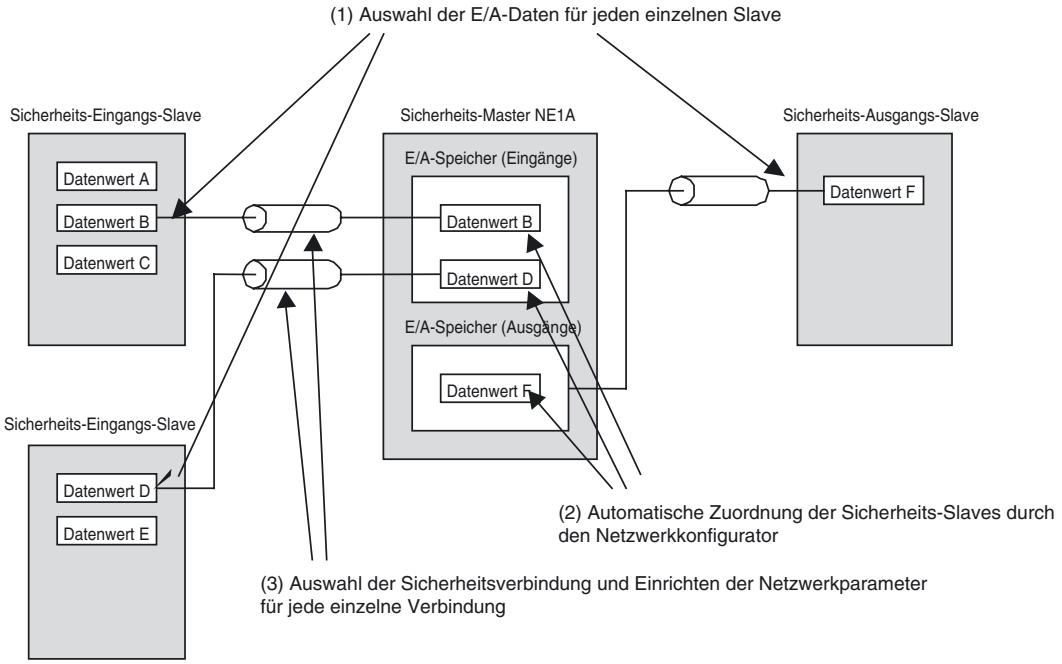
Mit dem Sicherheitsnetzwerk-Controller NE1A kommunizierende Sicherheits-Slaves werden auf Grundlage der mithilfe des Netzwerkkonfigurators vorgenommenen Einstellungen automatisch im E/A-Speicher des Sicherheitsnetzwerk-Controllers NE1A zugeordnet. Im Logik-Editor werden die E/A-Punkte registrierter Slaves als E/A-Tags angezeigt. Sie ermöglichen die Programmierung ohne Kenntnis der exakten Speicheradressen im Sicherheitsnetzwerk-Controller NE1A.

4-4-2 Einstellungen für Sicherheits-E/A-Verbindungen

Die Durchführung einer Sicherheits-E/A-Kommunikation zwischen dem Sicherheitsnetzwerk-Controller NE1A und den Sicherheits-Slaves erfordert, dass gewisse Einstellungen für Sicherheits-E/A-Verbindungen vorgenommen werden. Unter einer „Verbindung“ versteht man den logischen Kommunikationspfad zwischen Master und Slave.

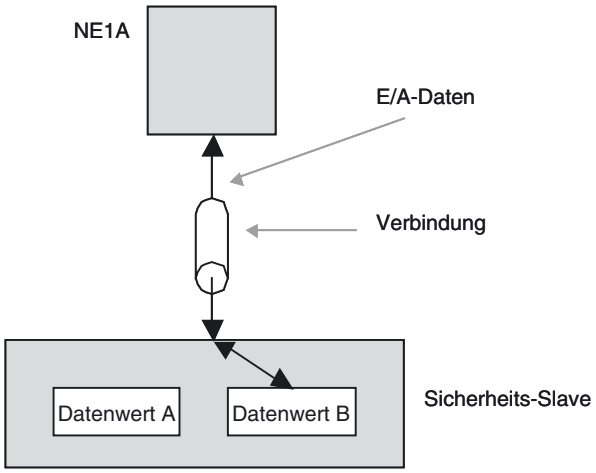
Im Einzelnen handelt es sich um die folgenden Einstellungen:

1. E/A-Verbindungs-Einstellungen (Auswahl der vom Slave verwendeten E/A-Daten)
2. Open Type
3. Connection Type
4. EPI (Expected Packet Interval)



Einstellungen für Sicherheits-E/A-Verbindungen

Manche Slaves verfügen intern über mehrere E/A-Daten-Sätze. Bei diesen Slaves muss ausgewählt werden, welche Daten bei der Kommunikation übertragen werden. Hierbei können die im Sicherheitsnetzwerk-Controller NE1A zuzuordnenden Daten aus den Daten des registrierten Sicherheits-Slaves ausgewählt werden.



Parameter „Open Type“

Die Einstellung dieses Parameters bestimmt die Vorgehensweise des Sicherheitsnetzwerk-Controllers NE1A beim Herstellen einer Verbindung.

Open Type	Beschreibung
Configure the Safety Slave	Beim Herstellen der Verbindung wird der Sicherheits-Slave konfiguriert.
Check the Safety Signature	Beim Herstellen der Verbindung wird die Sicherheitssignatur und damit die Integrität der Konfiguration des Sicherheits-Slaves überprüft.
Open Only	Beim Herstellen der Verbindung wird die Integrität der Konfiguration des Sicherheits-Slaves nicht überprüft.

⚠ VORSICHT

Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, ist stets darauf zu achten, dass der Sicherheits-Master oder Sicherheits-Slave die richtige Konfiguration aufweist, bevor „Open Type“ als *Open Only.* konfiguriert wird.

4-4-3 Parameter „Connection Type“

Für die Kommunikation mit Sicherheits-Slaves verwendeter Verbindungstyp.

Die nachstehende Tabelle erläutert die möglichen Einstellungen.

Verbindungsart	Beschreibung
Multi-cast Connection	Diese Verbindungsart kann nur verwendet werden, wenn es sich bei dem Slave um eine Sicherheits-Eingangs-Baugruppe handelt. Bei Verwendung einer Multicast-Verbindung kann eine Sicherheits-Eingangs-Baugruppe die Eingangsdaten an maximal 15 Sicherheitsnetzwerk-Controller NE1A übertragen. Alle als Sicherheits-Master fungierenden Sicherheitsnetzwerk-Controller NE1A, bei denen derselbe E/A-Datentyp für E/A-Verbindungen und derselbe EPI-Wert festgelegt wurde, werden als einer Multicast-Gruppe angehörig betrachtet. Diese Verbindungsart kann auch gewählt werden, wenn nur ein Sicherheitsnetzwerk-Controller NE1A im Netzwerk als Sicherheits-Master fungiert.
Single-cast Connection	Bei Auswahl dieses Verbindungstyps findet eine 1:1-Sicherheits-E/A-Kommunikation zwischen Sicherheits-Master und Sicherheits-Slave statt.

Parameter „EPI (Expected Packet Interval)“

Dieser Parameter bestimmt das Intervall, in dem die Sicherheitsdaten zwischen dem als Sicherheits-Master fungierenden Sicherheitsnetzwerk-Controller NE1A und den Sicherheits-Slaves übertragen werden. Mittels Zeitgebern wird überwacht, dass sendende Geräte ihre Daten innerhalb dieses Intervalls senden und empfangende Geräte normale Daten innerhalb dieses Intervalls empfangen. Werden innerhalb dieses Intervalls erwartete Daten nicht empfangen, wird die Verbindung getrennt und in den Sicherheitszustand gewechselt.

Hinweis

- Die hier eingestellte Zeit hat Auswirkungen auf die Netzwerkreaktionszeit. Informationen zur Netzwerkreaktionszeit finden Sie in den *Kapiteln 9, „Kommunikationsvermögen der dezentralen E/A und Ansprechzeit der lokalen E/A“* und *3, „Konstruktion eines Sicherheitsnetzwerks“*, des DeviceNet-Safety Konfigurationshandbuchs (Cat. No. Z905).
- Das für EPI eingestellte Minimum entspricht entweder der Zykluszeit des Sicherheitsnetzwerk-Controllers oder der Zykluszeit der Sicherheits-Slaves (immer 6 ms) - je nach dem, welcher Wert größer ist. Folglich betrifft es den für EPI eingestellten Mindestwert, wenn die Zykluszeit des Sicherheitsnetzwerk-Controllers länger ist als 6 ms.

4-4-4 Anhalten/Zurücksetzen der Kommunikation nach einem Fehler

Bei Controllern ab Geräteversion 1.0 kann der Benutzer festlegen, ob die E/A-Kommunikation angehalten oder fortgesetzt werden soll, wenn es während der Sicherheits-E/A-Kommunikation mit dem Sicherheits-Slave zu einer Zeitüberschreitung der Verbindung kommt. Wenn die E/A-Kommunikation wegen eines Zeitüberschreitungsfehlers angehalten wurde, kann sie über das Logik-Programm oder ein Programmiergerät neu gestartet werden.

Bei Controllern vor Version 1.0 wird die E/A-Kommunikation fortgesetzt (automatisches Wiederaufsetzen).

Einstellen des Betriebsmodus nach einem Kommunikationsfehler

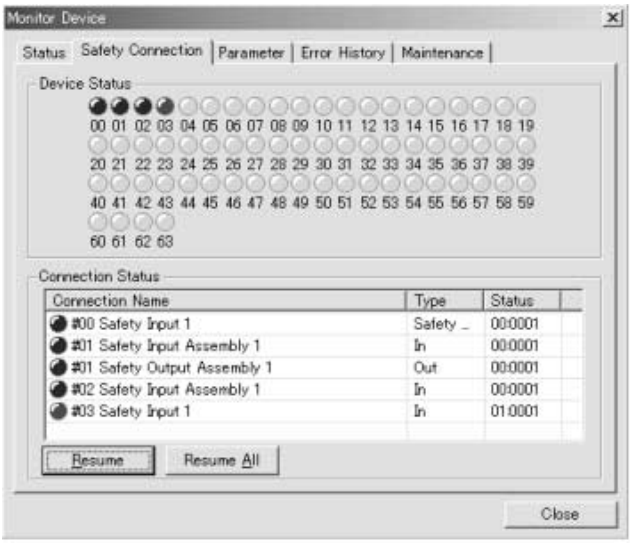
Für den Controller können folgende Betriebsmodi für den Fall festgelegt werden, dass es während der Sicherheits-E/A-Kommunikation mit dem Sicherheits-Slave zu einer Zeitüberschreitung kommt.

Modus nach Kommunikationsfehler	Beschreibung
Automatisches Wiederaufsetzen	Spezifizieren Sie diesen Modus, um die Sicherheits-E/A-Verbindung wiederherzustellen, wenn ein Fehler bei der Sicherheits-E/A-Kommunikation aufgetreten ist. Nachdem die Ursache für den Kommunikationsfehler beseitigt ist, startet die Sicherheits-E/A-Kommunikation automatisch neu.
Nur die Verbindung anhalten, an der der Fehler aufgetreten ist.	Spezifizieren Sie diesen Modus, um die Sicherheits-E/A-Kommunikation einer Verbindung anzuhalten, wenn ein Fehler bei der Sicherheits-E/A-Kommunikation aufgetreten ist. Die E/A-Kommunikation für normale Verbindungen wird fortgesetzt. Für den Neustart der Sicherheits-E/A-Kommunikation einer Verbindung, in der die E/A-Kommunikation angehalten wurde, übermitteln Sie einen entsprechenden Befehl mit dem Netzwerkkonfigurator. Sie können auch vorab eine Logik-Routine im Logik-Programm schreiben, um einen Neustart-Merker für die Sicherheits-E/A-Kommunikation zu aktivieren und die Kommunikation über ein bestimmtes Trigger-Bit neu zu starten.
Alle Verbindungen anhalten	Spezifizieren Sie diesen Modus, um die Sicherheits-E/A-Kommunikation mit allen Sicherheits-Slaves anzuhalten, wenn ein Fehler bei der Sicherheits-E/A-Kommunikation aufgetreten ist. Für den Neustart der Sicherheits-E/A-Kommunikation mit den Sicherheits-Slaves nach dem Anhalten der E/A-Kommunikation übermitteln Sie einen entsprechenden Befehl mit dem Netzwerkkonfigurator. Sie können auch vorab eine Logik-Routine im Logik-Programm schreiben, um alle Neustart-Merker für die Sicherheits-E/A-Kommunikation zu aktivieren und die Kommunikation über ein bestimmtes Trigger-Bit neu zu starten.

Zurücksetzen einer Verbindung, die wegen eines Kommunikationsfehlers unterbrochen wurde

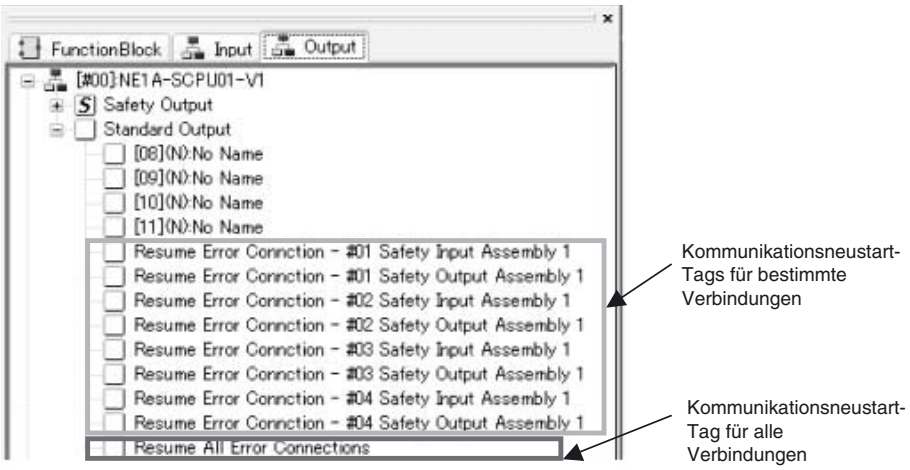
Wenn die E/A-Kommunikation einer Verbindung wegen einer Zeitüberschreitung angehalten wurde, kann sie neu gestartet werden, indem der Rücksetzmerker für die Kommunikation im Logik-Programm aktiviert wird oder über den Netzwerkkonfigurator der Befehl zum Neustarten der Kommunikation gegeben wird. Wenn der Kommunikationsmodus des Controllers so konfiguriert ist, dass nach einem Kommunikationsfehler alle Verbindungen angehalten werden, kann die Kommunikation nicht in einer einzelnen Verbindung neu gestartet werden. Führen Sie in diesem Fall einen Neustart der Kommunikation in allen Verbindungen durch.

1. Neustart der E/A-Kommunikation über den Netzwerkkonfigurator
   Stellen Sie eine Online-Verbindung mit dem Netzwerkkonfigurator her, markieren Sie den Sicherheits-Master, klicken Sie mit der rechten Maustaste, um das Popup-Menü anzuzeigen, und wählen Sie den Eintrag ***Monitor***, um das Fenster „Monitor Device“ anzuzeigen. Das folgende Fenster wird angezeigt, wenn die Registerkarte „Sicherheitsverbindung“ angeklickt wird.



Die Kommunikation kann für eine Verbindung neu gestartet werden, in der ein Fehler aufgetreten ist (am Verbindungsstatus erkennbar), indem diese Verbindung markiert und dann auf die Schaltfläche **Resume** geklickt wird. Wenn auf die Schaltfläche **Resume All** geklickt wird, erfolgt ein Neustart der E/A-Kommunikation für alle Slaves, deren Kommunikation angehalten wurde.

2. Neustart der E/A-Kommunikation über das Logik-Programm
   Beim Festlegen der Sicherheitsverbindung werden folgende Ausgangs-Tags des Logik-Programms für die Verbindung angezeigt.


FunctionBlock
Input
Output
[#00]:NE1A-SCPU01-V1
Safety Output
Standard Output
[08](N):No Name
[09](N):No Name
[10](N):No Name
[11](N):No Name
Resume Error Connction - #01 Safety Input Assembly 1
Resume Error Connction - #01 Safety Output Assembly 1
Resume Error Connction - #02 Safety Input Assembly 1
Resume Error Connction - #02 Safety Output Assembly 1
Resume Error Connction - #03 Safety Input Assembly 1
Resume Error Connction - #03 Safety Output Assembly 1
Resume Error Connction - #04 Safety Input Assembly 1
Resume Error Connction - #04 Safety Output Assembly 1
Resume All Error Connections
Kommunikationsneustart-Tags für bestimmte Verbindungen
Kommunikationsneustart-Tag für alle Verbindungen

Wenn diese Tags zuvor im Logik-Programm als E/A-Kommunikationsneustartbedingungen gesetzt wurden, kann die E/A-Kommunikation mit diesen Tags neu gestartet werden, indem die jeweilige Bedingung aktiviert wird (AUS → EIN).

4-5 Sicherheits-Slave-Funktion

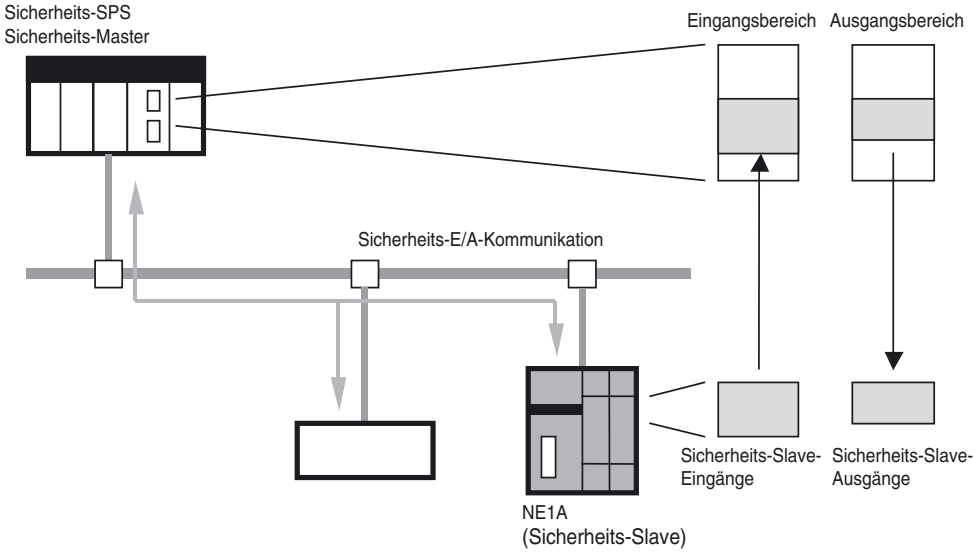
4-5-1 Sicherheits-E/A-Kommunikation bei Verwendung des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 als Sicherheits-Slave

Der Sicherheitsnetzwerk-Controller NE1A kann als Sicherheits-Slave fungieren.

Sicherheitsnetzwerk-Controller NE1A können gleichzeitig als Sicherheits-Master, als Sicherheits-Slave und als Standard-Slave fungieren.

Zur Nutzung des Sicherheitsnetzwerk-Controllers NE1A als Sicherheits-Slave müssen die folgenden Schritte durchgeführt werden:

1. Erstellung der E/A-Daten (Sicherheits-Slave-E/A) für die Verwendung als Sicherheits-Slave
2. Registrierung beim Sicherheits-Master
3. Festlegen der Einstellungen für die Sicherheits-E/A-Verbindungen im Sicherheits-Master



Spezifikationen bei Verwendung als Sicherheits-Slave

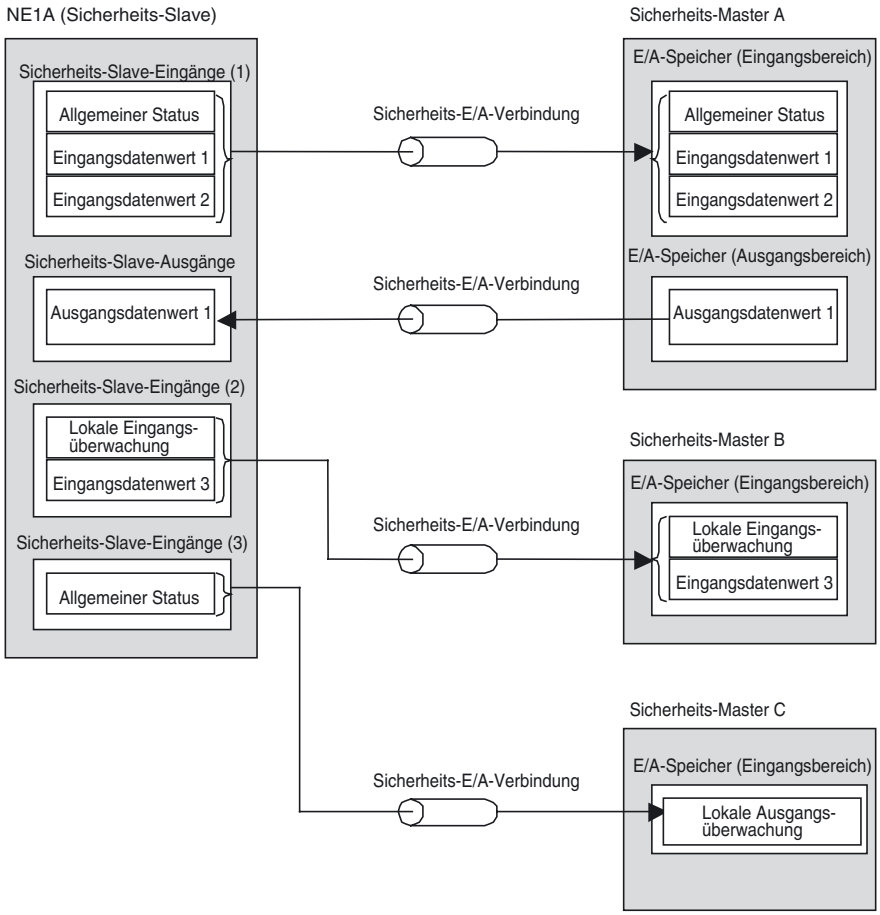
Sicherheits-E/A-Verbindungen	
Anzahl der Verbindungen	max. 4
Maximale Datengröße	16 Bytes Eingabedaten oder 16 Bytes Ausgabedaten (je Verbindung)
Verbindungstyp	Singlecast oder Multicast (siehe Hinweis)

Hinweis Über eine Multicast-Verbindung können Daten an bis zu 15 Master übertragen werden.

4-5-2 Erstellung der E/A-Daten (Sicherheits-Slave-E/A) für die Verwendung als Sicherheits-Slave

Zur Nutzung des Sicherheitsnetzwerk-Controllers NE1A als Sicherheits-Slave müssen E/A-Daten für den Sicherheits-Slave erstellt werden. Der Speicherblock für diese E/A-Daten wird als „Safety-Slave-E/A“ bezeichnet.

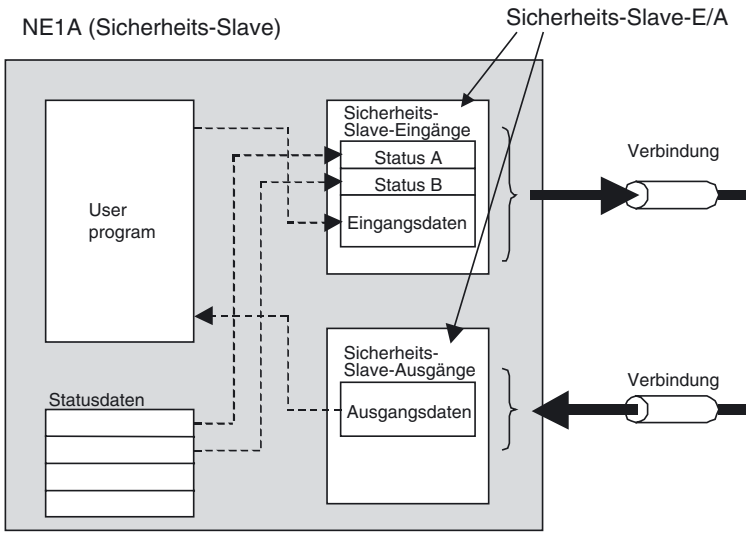
- Es können bis zu vier Arten von Safety-Slave-E/A erstellt werden.
- Die maximale Datengröße für die Safety-Slave-E/A beträgt 16 Bytes.
- Ist der Parameter „I/O Type“ der Safety-Slave-E/A auf „Safety Slave IN“ eingestellt, können die E/A-Daten auch die folgenden Statusinformationen beinhalten.
  - Allgemeiner Status
  - Status der lokalen Eingänge
  - Status der lokalen Ausgänge
  - Status der Testausgänge/Muting-Lampe
- Wenn der E/A-Typ für den Sicherheits-Slave bei einem Sicherheitsnetzwerk-Controller NE1A ab Version 1.0 „Slave IN“ lautet, können auch die folgenden Überwachungsdaten lokaler E/A in die E/A-Daten aufgenommen werden.
  - Lokale Eingangsüberwachung
  - Lokale Ausgangsüberwachung



Einstellung der Sicherheits-Slave-E/A

Die Einstellung der Sicherheits-Slave-E/A erfordert folgende Einstellungen:

1. Festlegen des E/A-Typs
2. Festlegen der E/A-Tags
3. Festlegen der zusätzlich zu übertragenden Statusinformationen
4. Festlegen der zusätzlichen Überwachungsdaten lokaler E/A



Festlegen des E/A-Typs (Parameter „I/O Type“)

E/A-Typ	Beschreibung
Sicherheits-Slave-Eingänge	Dateneingabe aus dem Netzwerk in den Sicherheits-Master
Safety Slave OUT	Datenausgabe aus dem Sicherheits-Master in das Netzwerk

Festlegen der E/A-Tags

Legen Sie die Eingangs- und Ausgangs-Datenblöcke der Sicherheits-Slave-E/A für die Verwendung im Anwenderprogramm fest. Für jede Sicherheits-Slave-E/A können mehrere Datenblöcke festgelegt werden. Folgende Größenangaben stehen für Datenblöcke zur Verfügung: BOOL (1 Byte), BYTE (1 Byte), WORD (2 Bytes) und DWORD (4 Bytes). Für jede Sicherheits-Slave-E/A können Datenblöcke bis zu einer Gesamtgröße von 16 Bytes festgelegt werden.

Die für die Datenblöcke definierten E/A-Tags können im Logik-Editor eingesetzt werden. Sie ermöglichen die Programmierung ohne Kenntnis der exakten Speicheradressen im Sicherheitsnetzwerk-Controller NE1A.

Festlegen der zusätzlich zu übertragenden Statusinformationen

Ist der Parameter „I/O Type“ der Sicherheits-Slave-E/A auf „Safety Slave IN“ eingestellt, können die folgenden Statusinformationen zur ersten Zeile der übertragenen Daten hinzugefügt werden. Einzelheiten zum jeweiligen Status finden Sie unter *4-3-3 Konfiguration der Daten des dezentralen E/A-Bereichs*.

Controller vor Version 1.0

Tag	Datengröße	Attribut
Allgemeiner Status	Byte	nicht sicher
Status der lokalen Eingänge	Wort	sicher
Status der lokalen Ausgänge	Byte	sicher
Status der Testausgänge/ Muting-Lampe	Byte	nicht sicher

Controller ab Version 1.0:

Tag	Datengröße	Attribut
Allgemeiner Status	Byte	nicht sicher
Status der lokalen Eingänge 1 bis N (siehe Hinweis)	Byte	Safety
Status der lokalen Ausgänge	Byte	Safety
Status der Testausgänge/Muting-Lampe 1 bis M (siehe Hinweis)	Byte	nicht sicher

Hinweis Bei NE1A-SCPU01-V1, N = 2 und M = 1. Bei NE1A-SCPU02 N = 5 und M = 2. Die Datengröße für den Status der lokalen Eingänge und den Status der Testausgänge-/Muting-Lampe kann in Byte angegeben werden.

Festlegen der lokalen E/A-Überwachungsdaten

Wenn der E/A-Typ der Sicherheits-Slave-E/A eines Sicherheitsnetzwerk-Controllers NE1A ab Version 1.0 „Slave IN“ lautet, können folgende Überwachungsdaten für lokale E/A hinter den Statusdaten in die Übertragungsdaten aufgenommen werden. Details zu Überwachungsdaten lokaler E/A finden Sie unter *4-3-3 Konfiguration der Daten des dezentralen E/A-Bereichs*.

Lokale E/A-Überwachung	Datengröße	Attribut
Überwachung der lokalen Eingänge 1 bis N (siehe Hinweis)	Byte	Safety
Überwachung der lokalen Ausgänge	Byte	Safety

Hinweis Für NE1A-SCPU01-V1 gilt N = 2. Für NE1A-SCPU02 gilt N = 5. Die Größe der Überwachungsdaten lokaler Eingänge kann in Bytes angegeben werden.

⚠ VORSICHT

Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, Bei der Generierung interner Statusdaten des Sicherheitsnetzwerk-Controllers NE1A mit dem Attribut „nicht sicher" werden die erforderlichen Maßnahmen für Sicherheitsdaten nicht ergriffen. Diese Daten dürfen daher nicht für die Konfiguration des Sicherheitssteuerungssystems eingesetzt werden.

4-6 Standard-Slave-Funktion

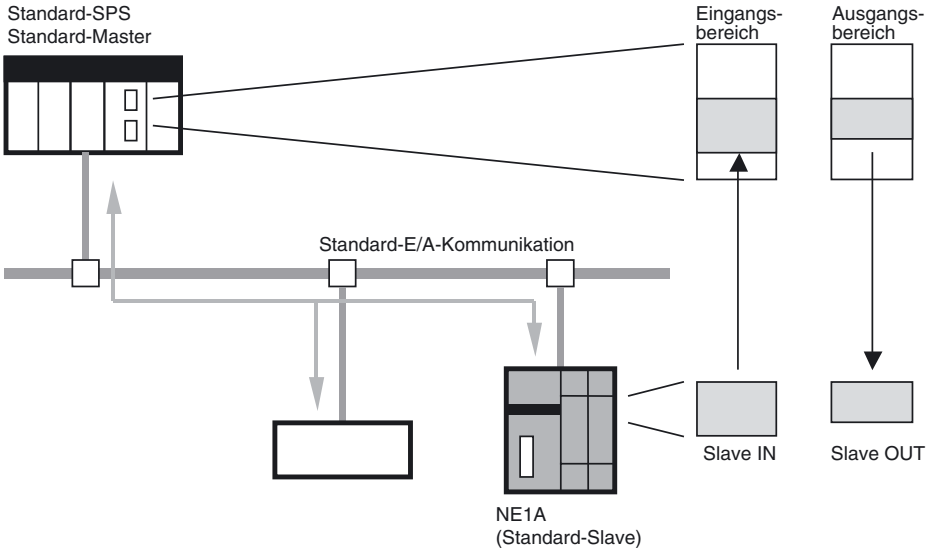
4-6-1 Sicherheits-E/A-Kommunikation bei Verwendung des Sicherheitsnetzwerk-Controllers NE1A als Standard-Slave

Der Sicherheitsnetzwerk-Controller NE1A kann als Standard-Slave fungieren. Sicherheitsnetzwerk-Controller NE1A können gleichzeitig als Sicherheits-Master, als Sicherheits-Slave und als Standard-Slave fungieren.

Die internen Statusinformationen des Sicherheitsnetzwerk-Controllers NE1A können von einer Standard-SPS aus überwacht werden, indem diese Informationen im Standard-Master zugeordnet werden.

Zur Nutzung eines Sicherheitsnetzwerk-Controllers NE1A als Standard-Slave müssen die folgenden Schritte durchgeführt werden:

1. Erstellung der E/A-Daten (Slave-E/A) für die Verwendung als Standard-Slave
2. Registrierung beim Standard-Master
3. Festlegen der Einstellungen für die E/A-Verbindungen im Standard-Master



Spezifikationen bei Verwendung als Standard-Slave

Standard-E/A-Verbindungen	
Anzahl der Verbindungen	max. 2
Maximale Datengröße	16 Bytes Eingabedaten oder 16 Bytes Ausgabedaten (je Verbindung) (siehe Hinweis 1)
Verbindungsart	Poll, Bitstrobe, COS oder Zyklisch

Hinweis

(1) Bei Verwendung einer Bitstrobe-Verbindung beträgt die maximale Datengröße 8 Bytes Eingabedaten und 0 Bytes Ausgabedaten.

(2) Die Verbindungsarten COS und Zyklisch können nicht gleichzeitig verwendet werden.

(3) Bei Auswahl von zwei Poll/COS oder Poll/Cyclic Verbindungen wird dasselbe Signalziel verwendet, sodass die maximale Ausgabedatengröße 16 Bytes beträgt. Bei Eingängen können bis zu 32 Datenbytes für 2 Verbindungen gesetzt werden.

4-6-2 Erstellung der E/A-Daten (Slave-E/A) für die Verwendung als Standard-Slave

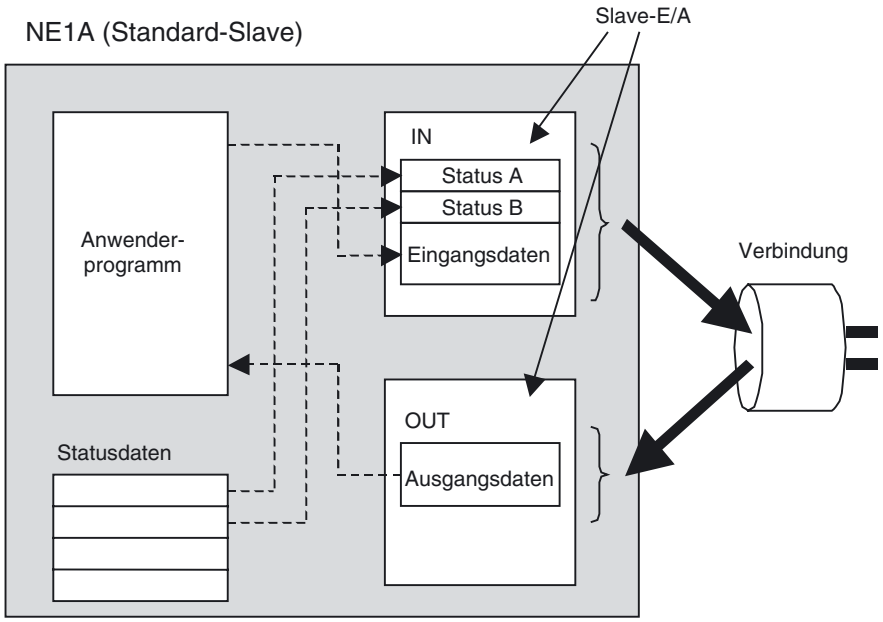
Zur Nutzung des Sicherheitsnetzwerk-Controllers NE1A als Standard-Slave müssen E/A-Daten für den DeviceNet-Slave erstellt werden. Die Speicherblöcke für diese E/A-Daten werden als „Slave-E/A“ bezeichnet.

- Es können für maximal zwei Verbindungen Slave-E/A-Blöcke erstellt werden.
- Die maximale Datengröße für die Slave-E/A beträgt 16 Bytes.
- Ist der Parameter „I/O Type“ der Slave-E/A auf „Slave IN“ eingestellt, können die E/A-Daten auch die folgenden Statusinformationen beinhalten.
  - Allgemeiner Status
  - Status der lokalen Eingänge
  - Status der lokalen Ausgänge
  - Status der Testausgänge/Muting-Lampe
- Wenn der E/A-Typ für den Sicherheits-Slave bei einem Sicherheitsnetzwerk-Controller NE1A ab Version 1.0 „Slave IN“ lautet, können auch die folgenden Überwachungsdaten lokaler E/A in die E/A-Daten aufgenommen werden.
  - Überwachung der lokalen Eingänge
  - Überwachung der lokalen Ausgänge

Einstellung der Slave-E/A

Die Einstellung der Slave-E/A erfordert folgende Einstellungen:

1. Festlegen der Verbindungsart
2. Festlegen der E/A-Tags
3. Festlegen der zusätzlich zu übertragenden Statusinformationen
4. Festlegen der zusätzlichen Überwachungsdaten lokaler E/A



Festlegen der Verbindungsart

Die vier in der folgenden Liste aufgeführten Verbindungsarten stehen zur Verfügung. Bei Verwendung einer Bitstrobe-Verbindung können keine Ausgangsdaten übertragen werden, da der Standard-Master keine Bitstrobe-Daten ausgeben kann. Die maximale Datengröße für Eingangsdaten beträgt bei einer Bitstrobe-Verbindung acht Bytes. Die Verbindungsarten COS und Zyklisch können nicht gleichzeitig verwendet werden.

- Poll
- Bitstrobe
- COS
- Zyklisch

Festlegen der E/A-Tags

Legen Sie die Eingangs- und Ausgangs-Datenblöcke der Slave-E/A für die Verwendung im Anwenderprogramm fest. Für jede Slave-E/A können mehrere Datenblöcke festgelegt werden. Folgende Größenangaben stehen für Datenblöcke zur Verfügung: BOOL (1 Byte), BYTE (1 Byte), WORD (2 Bytes) und DWORD (4 Bytes). Für jede Slave-E/A können Datenblöcke bis zu einer Gesamtgröße von 16 Bytes festgelegt werden.

Die für die Datenblöcke definierten E/A-Tags können im Logik-Editor eingesetzt werden. Sie ermöglichen die Programmierung ohne Kenntnis der exakten Speicheradressen im Sicherheitsnetzwerk-Controller NE1A.

Festlegen der zusätzlich zu übertragenden Statusinformationen

Ist der Parameter „I/O Type“ der Slave-E/A auf „Safety Slave IN“ eingestellt, können die folgenden Statusinformationen zur ersten Zeile der übertragenen Daten hinzugefügt werden. Einzelheiten zum jeweiligen Status finden Sie unter 4-3-3 *Konfiguration der Daten des dezentralen E/A-Bereichs*.

Controller vor Version 1.0

Tag	Datengröße
Allgemeiner Status	Byte
Status der lokalen Eingänge	Wort
Status der lokalen Ausgänge	Byte
Status der Testausgänge/Muting-Lampe	Byte

Controller ab Version 1.0:

Tag	Datengröße
Allgemeiner Status	Byte
Status der lokalen Eingänge 1 bis N (siehe Hinweis)	Byte
Status der lokalen Ausgänge	Byte
Status der Testausgänge/Muting-Lampe 1 bis N (siehe Hinweis)	Byte

Hinweis Bei NE1A-SCPU01-V1 gilt N = 2 und M = 1. Bei NE1A-SCPU02 gilt N = 5 und M = 2. Die Datengröße für den Status der lokalen Eingänge und den Status der Testausgänge-/Muting-Lampe kann in Byte angegeben werden.

Festlegen der lokalen E/A-Überwachungsdaten

Wenn der E/A-Typ der Sicherheits-Slave-E/A eines Sicherheitsnetzwerk-Controllers NE1A ab Version 1.0 „Slave IN“ lautet, können folgende Überwachungsdaten für lokale E/A hinter den Statusdaten in die Übertragungsdaten aufgenommen werden. Details zu Überwachungsdaten lokaler E/A finden Sie unter 4-3-3 *Konfiguration der Daten des dezentralen E/A-Bereichs*.

Überwachung der lokalen E/A	Datengröße
Überwachung der lokalen Eingänge 1 bis N (siehe Hinweis)	Byte
Überwachung der lokalen Ausgänge	Byte

Hinweis Bei NE1A-SCPU01-V1 gilt N = 2. Bei NE1A-SCPU02 gilt N = 5. Die Datengröße für den Status und die Überwachung der lokalen Eingänge kann in Byte angegeben werden.

⚠ VORSICHT

Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden.
Bei den durch Standard-E/A-Kommunikation übertragenen Datenattributen handelt es sich um Nicht-Sicherheits-Daten. Bei der Generierung dieser Daten werden die erforderlichen Maßnahmen für Sicherheitsdaten nicht ergriffen.
Diese Daten dürfen daher nicht für die Konfiguration des Sicherheitssteuerungssystems eingesetzt werden.

4-7 Explicit Message-Kommunikation

4-7-1 Empfangen von Explicit Messages

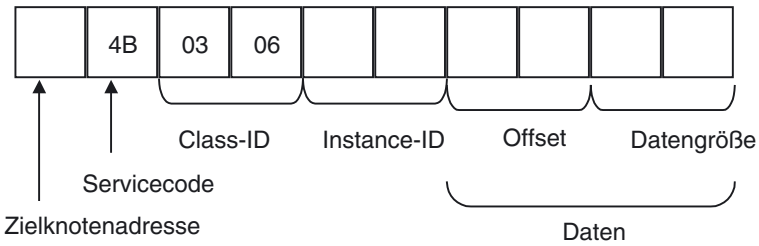
Explicit Messages ermöglichen Standard-Mastern den lesenden und schreibenden Zugriff auf sämtliche Daten und Parameter des Sicherheitsnetzwerk-Controllers NE1A. Der Controller empfängt vom Master gesendete Befehle und schickt eine entsprechende Antwort zurück.

Das folgende Beispiel illustriert den Lesedienst des Controllers für den E/A-Bereich. Einzelheiten zu verfügbaren Diensten finden Sie in *Anhang 3 DeviceNet Explicit Messages*.

NE1A I/O Area Read

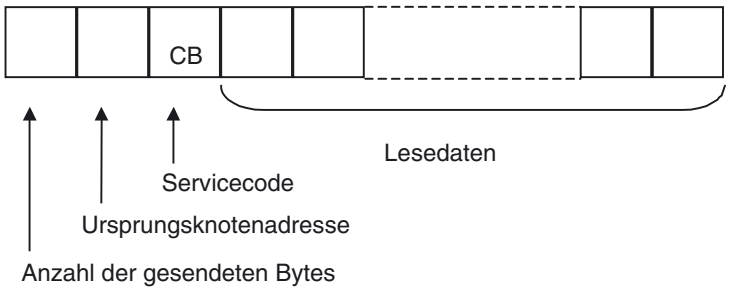
Auslesen der lokalen E/A-Punkte des Sicherheitsnetzwerk-Controllers NE1A oder des dem Sicherheitsnetzwerk-Controllers durch den Master zugeordneten Sicherheits-Slave-E/A-Bereichs.

Befehlsformat

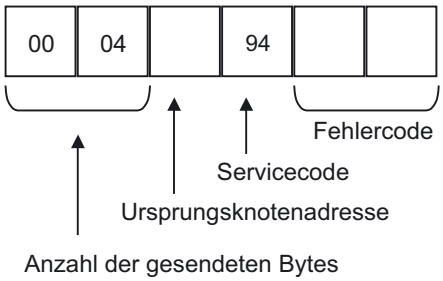


Antwortformat

- Normale Antwort auf die Explicit Message



- Fehlerantwort auf die Explicit Message



Zielknotenadresse (Befehl)

Knotenadresse des Sicherheitsnetzwerk-Controllers NE1A, dessen Daten gelesen werden sollen (1 Byte, Hexadezimalformat).

Servicecode (Befehl/Antwort)

Bei Befehlen: 4B (hex). Bei Antworten wird das höchstwertige Bit gesetzt und das Byte CB (hex) zrückgegeben.

Class-ID (Befehl)

0306 (hex)

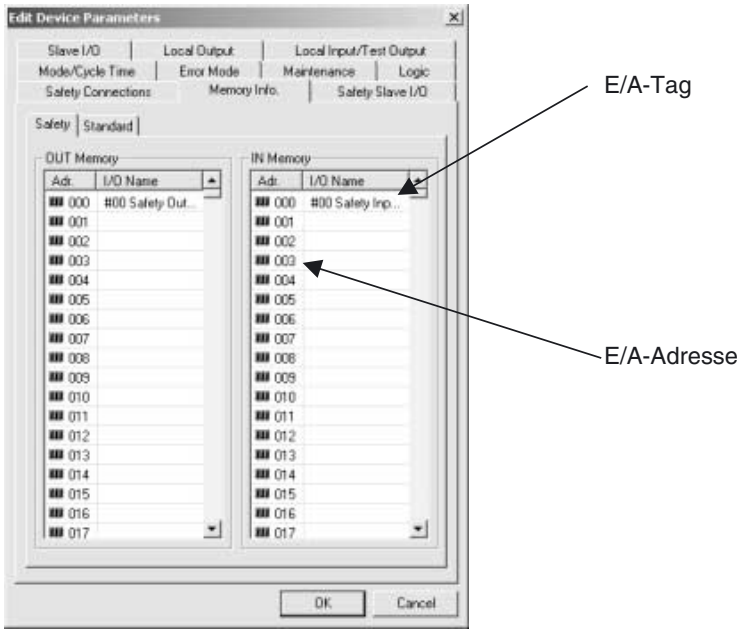
Instance-ID (Befehl)

Explicit Message	Dienst	Instance-ID
Lokalen Eingangsbereich lesen	Lesen	0001 (hex)
Lokalen Ausgangsbereich lesen	Lesen	0002 (hex)
Dezentralen Sicherheits-Eingangsbereich lesen	Lesen	0005 (hex)
Dezentralen Sicherheits-Ausgangsbereich lesen	Lesen	0006 (hex)

Daten (Befehl)

Offset	Adresse, ab der die Daten gelesen werden. Hierbei handelt es sich um den Byte-Offset, gerechnet ab der ersten Zeile des Bereichs.
Datengröße	Anzahl der zu lesenden Daten in Bytes (1 bis 256 Bytes).
Bereich	Lokaler Eingangsbereich: 0 oder 1 (Controller vor Version 1.0) 0 oder 1 (NE1A-SCPU01-V1) 0 bis 4 (NE1A-SCPU02) Lokaler Ausgangsbereich/Testausgangsbereich: 0 oder 1 Dezentraler Sicherheits-Eingangsbereich: 0 bis 511 Dezentraler Sicherheits-Ausgangsbereich: 0 bis 511

Auf der Registerkarte „Memory Info“ des Dialogfelds „Edit Device Parameters“ für den Sicherheitsnetzwerk-Controller NE1A können Sie die E/A-Adressen der gelesenen Speicherinformationen überprüfen.



Anzahl der gesendeten Bytes (Antwort)

Die Anzahl der vom anfordernden Quellknoten zu lesenden Datenbytes bis zum Ende der Antwort (Hexadezimalwert).

Ursprungsknotenadresse (Antwort)

Die Knotenadresse des antwortenden Sicherheitsnetzwerk-Controllers NE1A (1 Byte, Hexadezimalwert).

Lesedaten (Antwort)

E/A-Daten des angeforderten Bereichs.

Die nachstehenden Tabellen geben die Offsets und Bit-Zuordnungen der lokalen Eingänge und Ausgänge sowie der Testausgänge an.

- Lokale Eingänge (5 Bytes)

Offset (Bytes)	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Sicherheits-Eingangsklemme 7	Sicherheits-Eingangsklemme 6	Sicherheits-Eingangsklemme 5	Sicherheits-Eingangsklemme 4	Sicherheits-Eingangsklemme 3	Sicherheits-Eingangsklemme 2	Sicherheits-Eingangsklemme 1	Sicherheits-Eingangsklemme 0
1	Sicherheits-Eingangsklemme 15	Sicherheits-Eingangsklemme 14	Sicherheits-Eingangsklemme 13	Sicherheits-Eingangsklemme 12	Sicherheits-Eingangsklemme 11	Sicherheits-Eingangsklemme 10	Sicherheits-Eingangsklemme 9	Sicherheits-Eingangsklemme 8
2	Sicherheits-Eingangsklemme 23	Sicherheits-Eingangsklemme 22	Sicherheits-Eingangsklemme 21	Sicherheits-Eingangsklemme 20	Sicherheits-Eingangsklemme 19	Sicherheits-Eingangsklemme 18	Sicherheits-Eingangsklemme 17	Sicherheits-Eingangsklemme 16
3	Sicherheits-Eingangsklemme 31	Sicherheits-Eingangsklemme 30	Sicherheits-Eingangsklemme 29	Sicherheits-Eingangsklemme 28	Sicherheits-Eingangsklemme 27	Sicherheits-Eingangsklemme 26	Sicherheits-Eingangsklemme 25	Sicherheits-Eingangsklemme 24
4	Sicherheits-Eingangsklemme 39	Sicherheits-Eingangsklemme 38	Sicherheits-Eingangsklemme 37	Sicherheits-Eingangsklemme 36	Sicherheits-Eingangsklemme 35	Sicherheits-Eingangsklemme 34	Sicherheits-Eingangsklemme 33	Sicherheits-Eingangsklemme 32

Hinweis Bei NE1A-SCPU01 und NE1A-SCPU01-V1 kann der Status für 16 Klemmen gelesen werden (= Sicherheits-Eingangsklemmen 0 bis 15). Bei NE1A-SCPU02 kann der Status für 40 Klemmen gelesen werden (= Sicherheits-Eingangsklemmen 0 bis 39).

- Lokale Ausgänge und Testausgänge (2 Bytes)

Offset (Bytes)	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Sicherheits-Ausgangsklemme 7	Sicherheits-Ausgangsklemme 6	Sicherheits-Ausgangsklemme 5	Sicherheits-Ausgangsklemme 4	Sicherheits-Ausgangsklemme 3	Sicherheits-Ausgangsklemme 2	Sicherheits-Ausgangsklemme 1	Sicherheits-Ausgangsklemme 0
1	Test-Ausgangsklemme 7	Test-Ausgangsklemme 6	Test-Ausgangsklemme 5	Test-Ausgangsklemme 4	Test-Ausgangsklemme 3	Test-Ausgangsklemme 2	Test-Ausgangsklemme 1	Test-Ausgangsklemme 0

Hinweis Bei NE1A-SCPU01 und NE1A-SCPU01-V1 kann der Testausgangsstatus für 4 Klemmen gelesen werden (= Testausgangsklemmen 0 bis 3). Bei NE1A-SCPU02 kann der Testausgangsstatus für 8 Klemmen gelesen werden (= Testausgangsklemmen 0 bis 7).

Fehlercode (Antwort)

Die folgenden in DeviceNet definierten Fehlercodes können zurückgegeben werden.

Fehlercode	Fehlerbezeichnung	Ursache
08FF	Dienst wird nicht unterstützt	Fehler im Servicecode
13FF	Nicht genügend Daten	Die Datenmenge ist kürzer als die spezifizierte Menge
15FF	Zu viele Daten	Die Datenmenge ist größer als die spezifizierte Menge
16FF	Objekt ist nicht vorhanden	Die spezifizierte Klassen- oder Instanz-ID wird nicht unterstützt
20FF	Ungültiger Parameter	Die spezifizierten Operationsbefehlsdaten werden nicht unterstützt.

4-7-2 Explicit-Message-Übertragung

Der Sicherheitsnetzwerk-Controller NE1A kann aus dem Anwenderprogramm heraus Explicit Messages versenden.

Benutzerregistrierte Meldungen werden über das Netzwerk versendet, wenn bestimmte Trigger-Bedingungen erfüllt sind. Auf diese Weise können Überwachungs- und Steuerungsgeräte benachrichtigt oder Ausgänge für Anzeigen spezifiziert werden.

Die Bedingungen hierfür müssen mithilfe des Logik-Editors eingestellt werden.

Mit dem Sicherheitsnetzwerk-Controller NE1A können bis zu 32 Bytes Explicit-Message-Daten übertragen werden (siehe unten).

■ Explicit-Message-Datenformat

Parameterbezeichnung	Datengröße
MACID	1 Byte
Servicecode	1 Byte
Class-ID	2 Bytes
Instance-ID	2 Bytes
Servicedaten	0 bis 26 Bytes

Informationen zu Servicecodes, Klassen-IDs, Instanz-IDs und Servicedaten finden Sie im Handbuch für das jeweilige Zielgerät der Nachricht.

Vorgehensweise

Einstellen der Bedingungen für das Versenden von Explicit Messages.

1. Einstellung der Triggeradresse
   Auslöser für das Versenden der Explicit Message. Die Explicit Message wird versendet, wenn die eingestellte Adresse auf EIN gesetzt wird.
2. Einstellung der Sendebedingung
   Sendebedingungen für die Explicit Message. Die Anzahl der Wiederholungsversuche kann ebenfalls eingestellt werden.
3. Erstellung der zu versendenden Explicit Message
   Überprüfen Sie die Objektspezifikationen des Zielknotens und erstellen Sie basierend auf dem Explicit Message-Format die zu versendende Explicit Message.

Einschränkungen

- Im Anwenderprogramm kann nur eine Triggeradresse eingestellt werden.
- Der Sicherheitsnetzwerk-Controller NE1A schickt auf eine Explicit Message als Antwort den angeforderten Auszug aus seinem internen E/A-Speicher zurück. Beim Senden einer Explicit Message aus dem Anwenderprogramm des Sicherheitsnetzwerk-Controllers NE1A heraus können interne Informationen des Sicherheitsnetzwerk-Controllers NE1A nicht als Daten der zu versendenden Explicit Message genutzt werden.
- Daten aus Antworten auf vom Sicherheitsnetzwerk-Controller NE1A versendete Explicit Messages können im Anwenderprogramm des Sicherheitsnetzwerk-Controllers NE1A nicht verwendet werden.

⚠ VORSICHT

Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, dürfen Explicit-Message-Daten nicht als Sicherheitssignale verwendet werden.

Bei der Explicit Message-Kommunikation werden keine der für die Sicherheitskommunikation erforderlichen Maßnahmen getroffen.

Hinweis Detaillierte Informationen zu den Parametern von Explicit Messages entnehmen Sie bitte den DeviceNet-Spezifikationen.

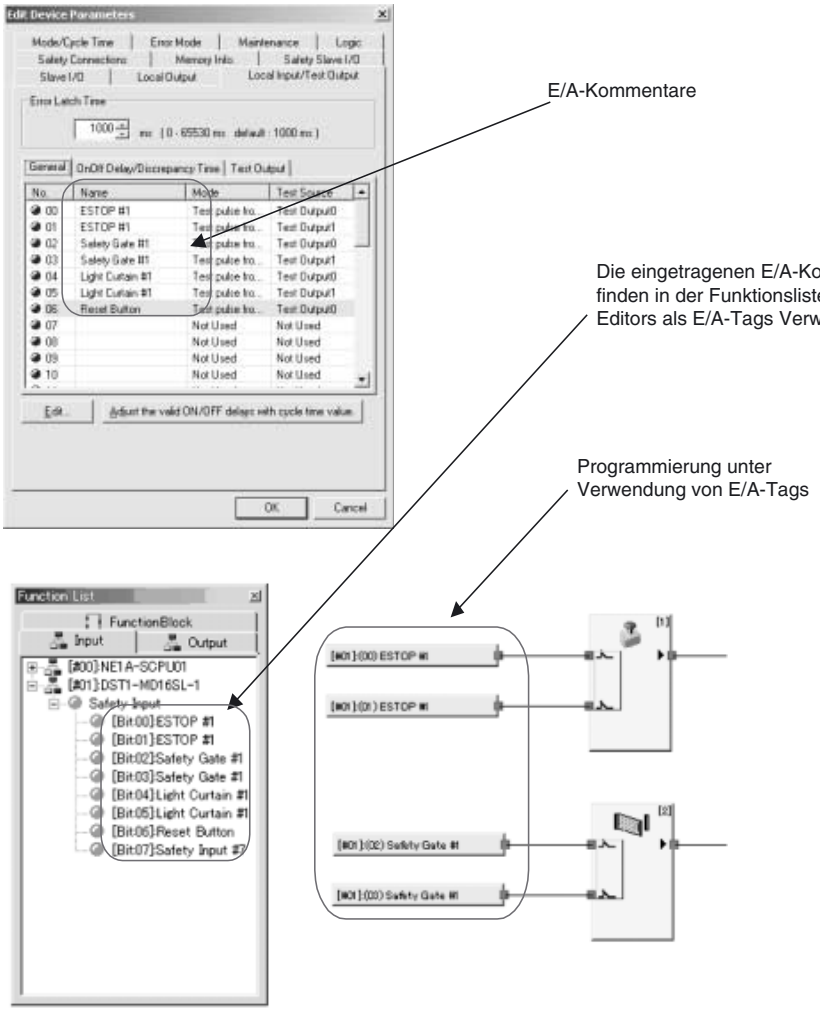
ABSCHNITT 5
E/A-Steuerung

5-1 Allgemeine Funktionen 90
5-1-1 E/A-Kommentare 90
5-1-2 Überwachung der E/A-Versorgungsspannung 91
5-1-3 Schalthäufigkeitszähler 91
5-1-4 Gesamteinschaltdauer-Überwachung 93
5-2 Sicherheitseingänge 97
5-2-1 Übersicht 97
5-2-2 Betriebsart der lokalen Sicherheitseingänge (Parameter) 98
5-2-3 Test Source (Parameter) 98
5-2-4 Eingangsverzögerungen (Einschalt- und Ausschaltverzögerungen) 98
5-2-5 Dual Channel Mode (Parameter) 99
5-2-6 Fehlerbehandlung 101
5-3 Testausgänge 102
5-3-1 Test Output Mode (Parameter) 102
5-3-2 Fehlerbehandlung 102
5-4 Sicherheitsausgänge 103
5-4-1 Übersicht 103
5-4-2 Output Channel Mode (Parameter) 103
5-4-3 Dual Channel Mode (Parameter) 103
5-4-4 Fehlerbehandlung 104

5-1 Allgemeine Funktionen

5-1-1 E/A-Kommentare

Jeder E/A-Klemme kann mithilfe des Netzwerkkonfigurators ein maximal 32 Zeichen langer Name zugeordnet und im Sicherheitsnetzwerk-Controller NE1A registriert werden. Diese E/A-Kommentare können in der Funktionsliste des Logik-Editors als E/A-Tags genutzt werden. E/A-Tags ermöglichen übersichtliche, anschauliche Programme, in denen problemlos ersichtlich ist, was an welcher Stelle wie gesteuert wird.



5-1-2 Überwachung der E/A-Versorgungsspannung

Der Sicherheitsnetzwerk-Controller NE1A-SCPU01 ermöglicht die Überwachung der E/A-Versorgungsspannung. Ist mindestens eine der E/A-Klemmen des Sicherheitsnetzwerk-Controllers NE1A auf eine andere Funktion als *Nicht verwendet* eingestellt und liegt keine E/A-Versorgungsspannung an, zeigt die Siebensegmentanzeige eine der folgenden Meldungen:

- Eingangs-Versorgungsspannung liegt nicht an: P4
- Ausgangs-Versorgungsspannung liegt nicht an: P5

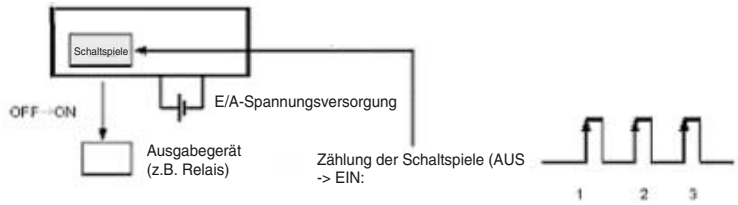
Der Status der E/A-Versorgungsspannung kann auch mittels DeviceNet-Kommunikation (Allgemeiner Status) abgefragt werden.

5-1-3 Schalthäufigkeitszähler

Übersicht

Beim Sicherheitsnetzwerk-Controller NE1A ab Version 1.0 zählt diese Funktion die Anzahl der Einschaltvorgänge (AUS → EIN) eines lokalen Eingangs, Testausgangs oder lokalen Ausgangs und speichert den Zählerwert im nichtflüchtigen Speicher.

- Zählbereich: 0 bis 4.294.967.295 Schaltspiele (gespeichert als 00000000 bis FFFFFFFF Hex)
- Zähleinheit: Schaltspiele
- Auflösung: Je nach Zyklusdauer



Diese Information können mithilfe des Netzwerkkonfigurators oder mit Explicit Messages überwacht werden.

Hinweis

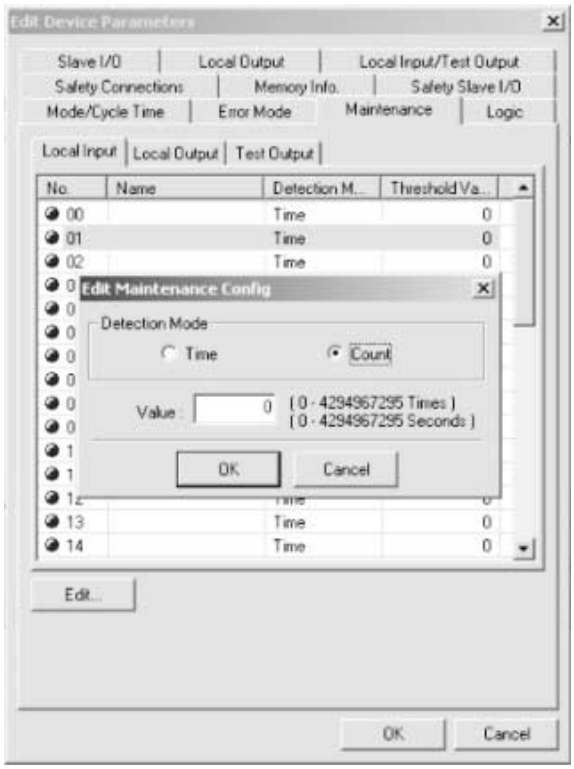
(1) Schalthäufigkeitszählung (Count) und Gesamteinschaltdauer-Überwachung (Time) können nicht gleichzeitig für ein Bit verwendet werden. Wählen Sie eine der beiden Funktionen über die Einstellung „Maintenance Counter Mode Choice“ aus.

(2) Bei einem Wechsel der Einstellung „Maintenance Counter Mode Choice“ werden die gesammelten Daten (Schalthäufigkeit oder Gesamteinschaltdauer) gelöscht.

(3) Die Erfassung der Schalthäufigkeit bzw. der Gesamteinschaltdauer ist außer Funktion, wenn die E/A-Spannungsversorgung ausgeschaltet ist.

Einstellung des Schaltspielalarm-Schwellenwerts mittels Netzwerkkonfigurator

Wartungsmodus (Maintenance Counter Mode Choice) und Alarmschwellenwert (Threshold Maintenance Counter) können für jeden lokalen Eingang, Testausgang und lokalen Ausgang festgelegt werden.

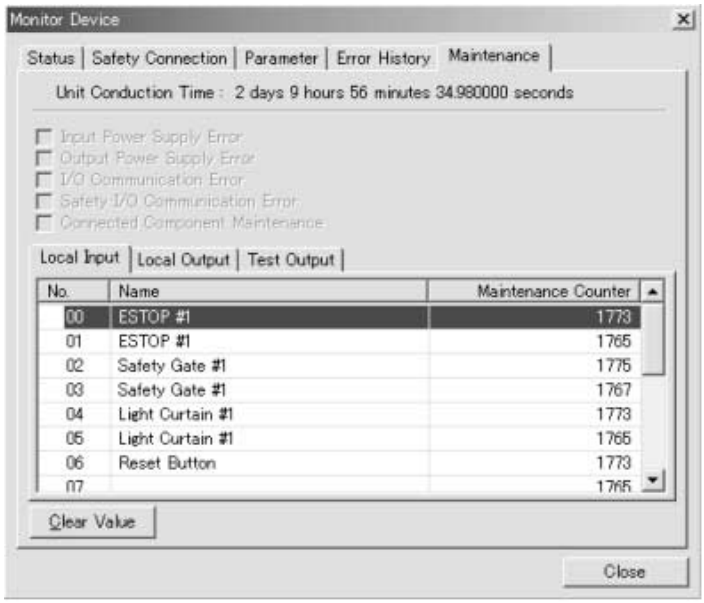


Wenn der Alarmschwellenwert (Threshold Maintenance Counter) auf 0 gesetzt wird, vergleicht der Controller den Zähler- oder Zeit-Istwert nicht mit dem Alarmsollwert.

Schaltspielüberwachung mittels Netzwerkkonfigurator

Die nachstehend aufgeführten Methoden eignen sich alle zur Überwachung der Schaltspielanzahl im lokalen Eingangsstatus, Testausgangsstatus oder lokalen Ausgangsstatus.

1. Markieren Sie das Gerät, und wählen Sie den Eintrag ***Device Maintenance Information*** aus der Menüleiste.
2. Markieren Sie das Gerät, und klicken Sie in der Werkzeugleiste auf die Schaltfläche **Maintenance**.
3. Markieren Sie das Gerät, klicken Sie mit der rechten Maustaste darauf, und wählen Sie den Eintrag ***Maintenance information*** aus dem Popup-Menü.
4. Markieren Sie das Gerät, wählen Sie den Eintrag ***Device – Monitor*** aus der Menüleiste, und klicken Sie im angezeigten Fenster auf die Registerkarte **Maintenance**.
5. Markieren Sie das Gerät, klicken Sie in der Werkzeugleiste auf die Schaltfläche **Device Monitor**, und klicken Sie im angezeigten Fenster auf die Registerkarte **Maintenance**.
6. Markieren Sie das Gerät, klicken Sie mit der rechten Maustaste darauf, wählen Sie den Eintrag ***Monitor*** aus dem Popup-Menü, und klicken Sie im angezeigten Fenster auf die Registerkarte **Maintenance**.



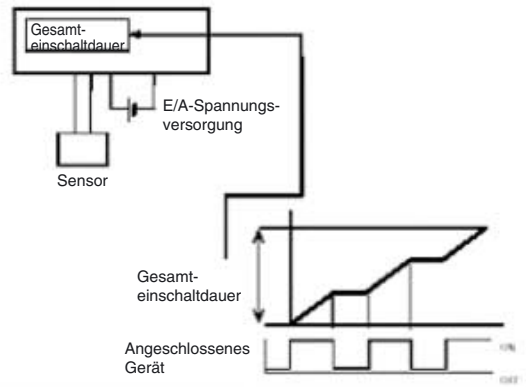
Der Schaltspiel-Zählerwert eines jeden E/A-Punkts kann gelöscht werden. Zum Löschen des Zählerwerts markieren Sie den zu löschenden Schaltspielzähler und klicken auf die Schaltfläche **Clear Value**.

5-1-4 Gesamteinschaltdauer-Überwachung

Übersicht

Beim Sicherheitsnetzwerk-Controller NE1A ab Version 1.0 zählt diese Funktion, wie lange ein lokaler Eingang, Testausgang oder lokaler Ausgang aktiviert ist (EIN), und speichert die Gesamteinschaltdauer im nichtflüchtigen Speicher.

- Zählbereich: 0 bis 4.294.967.295 Sekunden (gespeichert als 00000000 bis FFFFFFFF Hex)
- Zähleinheit: Sekunden



Diese Information können mithilfe des Netzwerkkonfigurators oder mit Explicit Messages überwacht werden.

Hinweis

(1) Gesamteinschaltdauer-Überwachung (Time) und Schalthäufigkeitszählung (Count) können nicht gleichzeitig für ein Bit verwendet werden. Wählen Sie eine der beiden Funktionen über die Einstellung „Maintenance Counter Mode Choice“ aus.

(2) Bei einem Wechsel der Einstellung „Maintenance Counter Mode Choice“ werden die gesammelten Daten (Schalthäufigkeit oder Gesamteinschaltdauer) gelöscht.

(3) Die Erfassung der Schalthäufigkeit bzw. der Gesamteinschaltdauer ist außer Funktion, wenn die E/A-Spannungsversorgung ausgeschaltet ist.

(4) Die Gesamteinschaltdauer-Überwachung prüft in Abständen von einer Sekunde, ob das angeschlossene Gerät aktiviert ist (EIN). Falls die Einschaltintervalle des Geräts kürzer sind als eine Sekunde, wird die Gesamteinschaltdauer möglicherweise nicht exakt gemessen.

■ **Berechnung der Gesamteinschaltdauer anhand halbsekündiger Einschaltimpulse (0,5 s)**

In Abbildung A beträgt die tatsächliche Einschaltdauer des Bits 0,5 s × 3 = 1,5 s, jedoch ist das Bit nur einmal während einer Statusüberprüfung aktiviert (EIN), weshalb eine Gesamteinschaltdauer von 1 s gemessen wird.

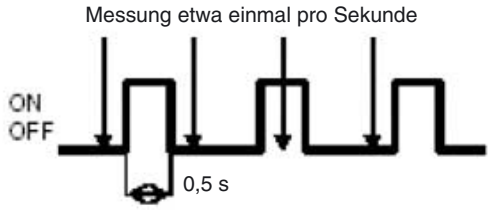


Abbildung A

In Abbildung B beträgt die tatsächliche Einschaltdauer des Bits 0,5 s × 3 = 1,5 s, jedoch ist das Bit zweimal während einer Statusüberprüfung aktiviert (EIN), weshalb eine Gesamteinschaltdauer von 2 s gemessen wird.

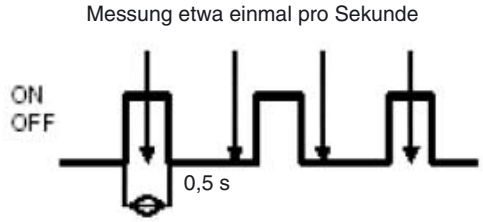


Abbildung B

■ **Berechnung der Gesamteinschaltdauer anhand anderthalbsekündiger Einschaltimpulse (1,5 s)**

In Abbildung C beträgt die tatsächliche Einschaltdauer des Bits 1,5 s × 2 = 3 s, jedoch ist das Bit viermal während einer Statusüberprüfung aktiviert (EIN), weshalb eine Gesamteinschaltdauer von 4 s gemessen wird.

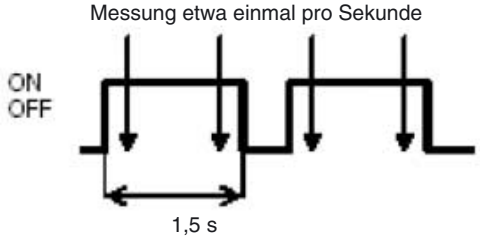
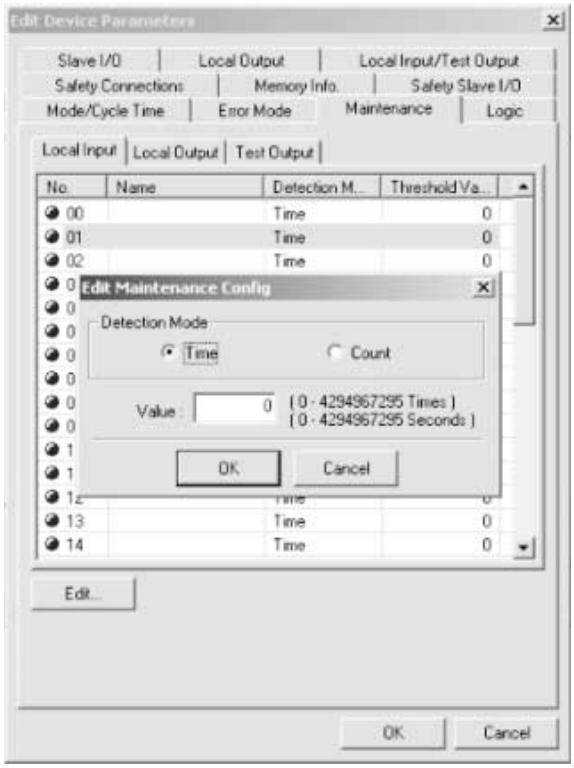


Abbildung C

Einstellung des Gesamteinschaltdauer-Alarmschwellenwerts mittels Netzwerkkonfigurator

Wartungsmodus (Maintenance Counter Mode Choice) und Alarmschwellenwert (Threshold Maintenance Counter) können für jeden lokalen Eingang, Testausgang und lokalen Ausgang festgelegt werden.

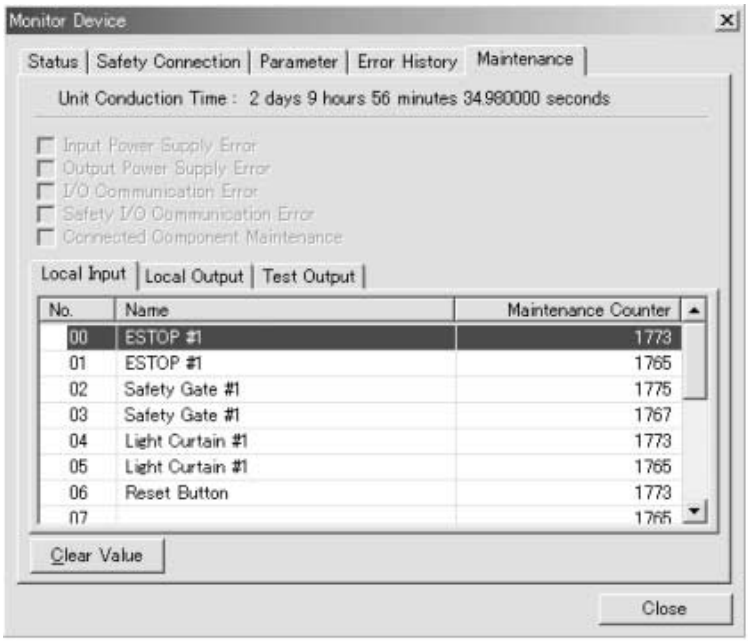


Wenn der Alarmschwellenwert (Threshold Maintenance Counter) auf 0 gesetzt wird, vergleicht der Controller den Zähler- oder Zeit-Istwert nicht mit dem Alarmsollwert.

Überwachung der Gesamteinschaltdauer mittels Netzwerkkonfigurator

Die nachstehend aufgeführten Methoden eignen sich alle zur Überwachung der Gesamteinschaltdauer im lokalen Eingangsstatus, Testausgangsstatus oder lokalen Ausgangsstatus.

1. Markieren Sie das Gerät, und wählen Sie den Eintrag ***Device Maintenance Information*** aus der Menüleiste.
2. Markieren Sie das Gerät, und klicken Sie in der Werkzeugleiste auf die Schaltfläche **Maintenance**.
3. Markieren Sie das Gerät, klicken Sie mit der rechten Maustaste darauf, und wählen Sie den Eintrag ***Maintenance information*** aus dem Popup-Menü.
4. Markieren Sie das Gerät, wählen Sie den Eintrag ***Device – Monitor*** aus der Menüleiste, und klicken Sie im angezeigten Fenster auf die Registerkarte **Maintenance**.
5. Markieren Sie das Gerät, klicken Sie in der Werkzeugleiste auf die Schaltfläche **Device Monitor**, und klicken Sie im angezeigten Fenster auf die Registerkarte **Maintenance**.
6. Markieren Sie das Gerät, klicken Sie mit der rechten Maustaste darauf, wählen Sie den Eintrag ***Monitor*** aus dem Popup-Menü, und klicken Sie im angezeigten Fenster auf die Registerkarte **Maintenance**.



Der Gesamteinschaltdauer-Zählerwert eines jeden E/A-Punkts kann gelöscht werden. Zum Löschen des Zeitwerts markieren Sie die zu löschende Gesamteinschaltdauer und klicken auf die Schaltfläche **Clear Value**.

5-2 Sicherheitseingänge

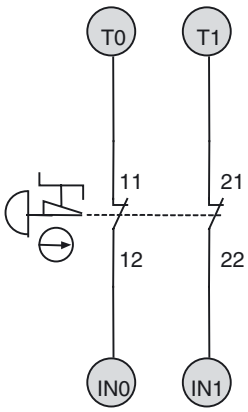
5-2-1 Übersicht

Der Sicherheitsnetzwerk-Controller NE1A-SCPU01(-V1) ist mit 16 Sicherheitseingängen ausgestattet.
Der Sicherheitsnetzwerk-Controller NE1A-SCPU02 ist mit 40 Sicherheitseingängen ausgestattet.
Durch Einrichtung und Verdrahtung entsprechend der Art der anzuschließenden Eingangsgeräte oder des zu erreichenden Sicherheitsniveaus kann der Sicherheitsnetzwerk-Controller NE1A flexibel für die verschiedensten Anwendungen eingesetzt werden. Nachstehend finden Sie einige Beispiele für die Verwendung der Sicherheitseingänge des Sicherheitsnetzwerk-Controllers NE1A.

Anschluss von Sicherheitsgeräten mit Kontaktausgängen

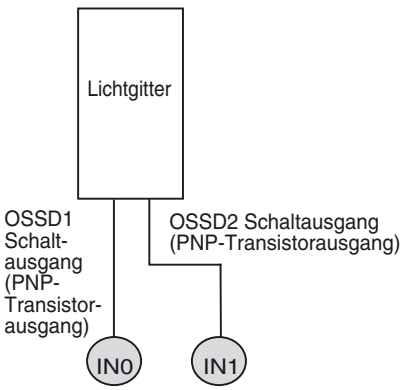
Das vom Testausgang (Impulsausgang) ausgegebene Signal wird über den Schaltkontakt eines Sicherheitsgeräts in den Sicherheitseingang geführt. Durch Analyse des am Sicherheitseingang anliegenden Signals, das im Normalfall dem Testimpulssignal entsprechen muss, lassen sich Fehler in der Eingangssignalleitung feststellen:

- Kurzschluss zur Versorgungsspannung (positive Seite)
- Erdschlüsse
- Querschluss zwischen Eingangssignalleitungen



Anschluss von Sicherheitsgeräten mit Halbleiterausgängen

Das Ausgangssignal eines Sicherheitsgeräts mit 24-V-DC-Halbleiterausgang (z. B. der Schaltausgang eines Lichtgitters) wird an den Sicherheitseingang angeschlossen. Fehler in der Ausgangssignalleitung des Schaltausgangs (d. h. der Eingangssignalleitung des Sicherheitsnetzwerk-Controllers NE1A) werden von dem extern angeschlossenen Gerät (z.B. Lichtgitter) festgestellt.



5-2-2 Betriebsart der lokalen Sicherheitseingänge (Parameter)

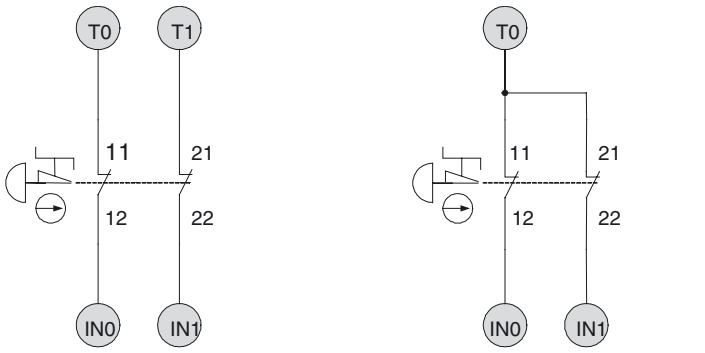
Je nach angeschlossenem externem Gerät muss der Parameter „Input Channel Mode“ (Betriebsart für die lokalen Sicherheitseingänge) entsprechend gesetzt werden. Details zu den Betriebsarten finden Sie in der nachstehenden Tabelle.

Einstellung	Beschreibung
Not used	An diesen Eingang ist kein externes Gerät angeschlossen.
Test pulse from test output	Dieser Eingang ist über ein Sicherheitsgerät mit Kontaktausgang mit einem Testausgang verbunden. Bei Auswahl dieses Modus muss für den Parameter „Test Source“ der als Testquelle zu verwendende Testausgang ausgewählt und der Parameter „Test Output Mode“ dieses Testausgangs auf *Pulse Test Output* eingestellt werden. Auf diese Weise können Kurzschlüsse mit der Versorgungsspannungsleitung, Erdschlüsse sowie Querschlüsse zwischen Eingangssignalleitungen erkannt werden.
Used as a safety input	An diesen Eingang ist ein Sicherheitsgerät mit Halbleiterausgang (z. B. Lichtgitter) angeschlossen.
Used as a standard input	An diesen Eingang ist ein Standardgerät (d. h. ein nicht sicheres Gerät) angeschlossen.

5-2-3 Test Source (Parameter)

Ist der Parameter „Input Channel Mode“ eines Sicherheitseingangs auf „Test Pulse from Test Out“ eingestellt, muss der Parameter „Test Source“ auf den in Verbindung mit dem Sicherheitseingang zu verwendenden *Testausgang eingestellt werden.* Ist eine Erkennung von Querschlüssen zwischen Eingangsleitungen erforderlich, muss für jede in diesem Modus betriebene Eingangsleitung ein anderer Testausgang bestimmt werden.

Beispiele:



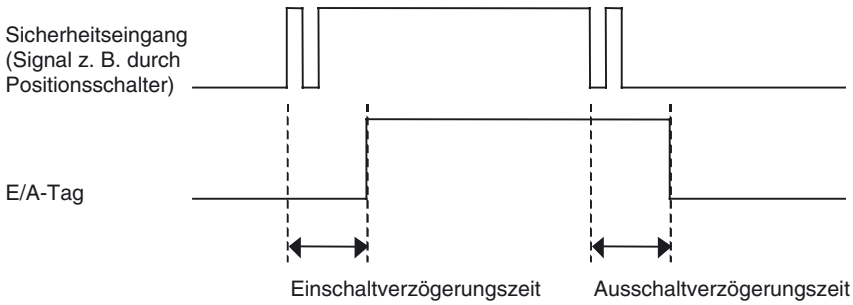
Querschlusserkennung zwischen Eingangssignalleitungen ist erforderlich.

Querschlusserkennung zwischen Eingangssignalleitungen ist nicht erforderlich.

Hinweis Bei NE1A-SCPU02 können die Klemmen T0 bis T3 als Testquellen für IN0 bis IN19 festgelegt werden. Die Klemmen T4 bis T7 können als Testquellen für IN20 bis IN39 festgelegt werden.

5-2-4 Eingangsverzögerungen (Einschalt- und Ausschaltverzögerungen)

Für die lokalen Sicherheitseingänge des Sicherheitsnetzwerk-Controllers NE1A können Verzögerungszeiten zwischen 0 und 126 ms (jeweils als Vielfache der Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A) eingestellt werden. Diese Eingangsverzögerungen erleichtern die Unterdrückung von Kontaktprellen und Störeinflüssen.



WICHTIG Beide Eingangsverzögerungen (Einschalt- und Ausschaltverzögerung) müssen zur E/A-Ansprechzeit hinzugerechnet werden und haben somit Auswirkungen auf die Berechnung des Sicherheitsabstands.
Details hierzu finden Sie in *Kapitel 9 Kommunikationsvermögen der dezentralen E/A und Ansprechzeit der lokalen E/A*.

5-2-5 Dual Channel Mode (Parameter)

Die lokalen Sicherheitseingänge des Sicherheitsnetzwerk-Controllers NE1A können paarweise im Zweikanalmodus betrieben werden. Dieser Modus bietet die folgenden Möglichkeiten:

- Der Status der beiden Eingänge kann bestimmt und in E/A-Tags abgebildet werden.
- Die Zeitabweichung zwischen der Änderung des Zustands eines der beiden Eingänge bis zur Änderung des Zustands des anderen Eingangs kann ermittelt und ausgewertet werden.

Einstellung	Beschreibung
Single Channel	Der Eingang wird als unabhängiger Sicherheitseingang verwendet.
Dual Channel Equivalent	Betrieb des Sicherheitseingangs in Verbindung mit einem zweiten Sicherheitseingang im Zweikanal-Äquivalenzmodus.
Dual Channel Complementary	Betrieb des Sicherheitseingangs in Verbindung mit einem zweiten Sicherheitseingang im Zweikanal-Komplementärmodus.

Abbildung des Zustands der Eingänge in E/A-Tags

Die nachstehenden Tabellen erläutern, wie der Status der Sicherheitseingänge im Ein- und Zweikanalmodus auf die entsprechenden E/A-Tags abgebildet wird.

Modus	Eingangszustand an der Sicherheitseingangsklemme	E/A-Tag	Bedeutung
	IN (x)	IN (x)	
Single Channel	0	0	AUS
	1	1	EIN

X = 0 bis 15 (NE1A-SCPU01(-V1))
X = 0 bis 39 (NE1A-SCPU02)

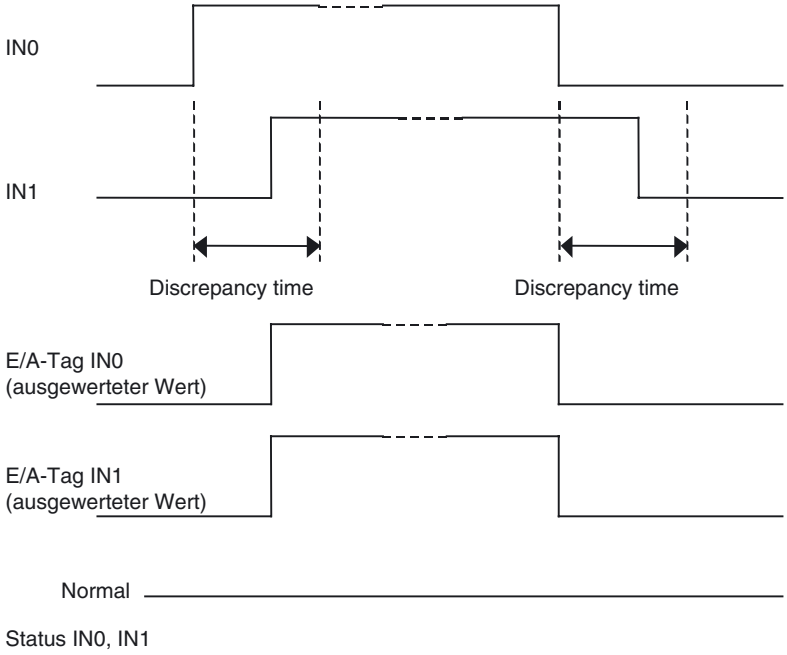
Einstellung	Eingangszustand an der Sicherheitseingangsklemme		E/A-Tag		Bedeutung
	IN (n)	IN (n+1)	IN (n)	IN (n+1)	
Dual Channel Equivalent	0	0	0	0	AUS
	0	1	0	0	abweichend
	1	0	0	0	abweichend
	1	1	1	1	EIN
Dual Channel Complementary	0	0	0	1	abweichend
	0	1	0	1	AUS
	1	0	1	0	EIN
	1	1	0	1	abweichend

n = Gerade Zahl

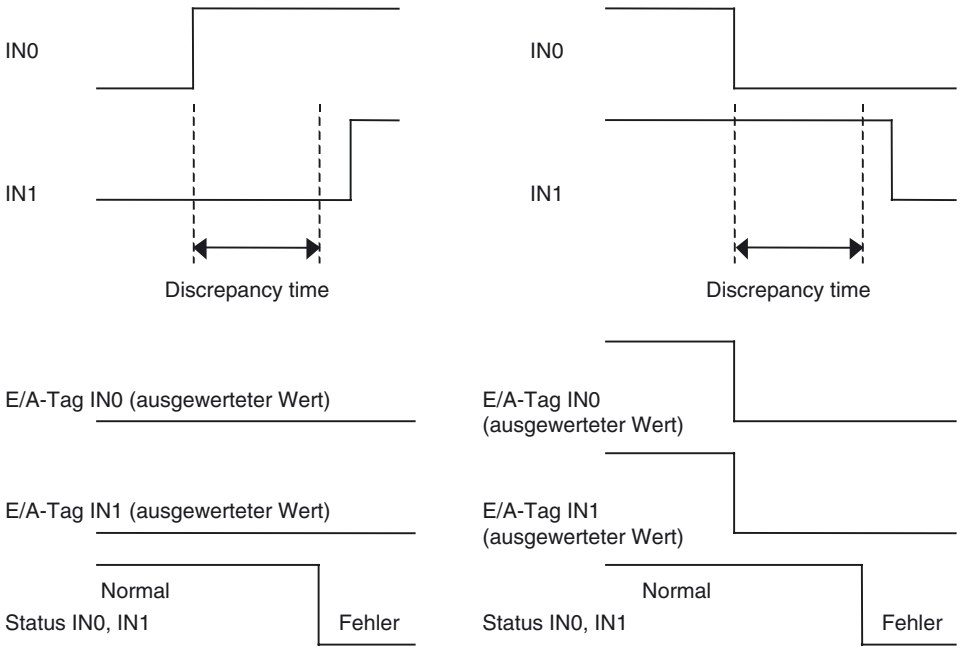
Diskrepanzzeit

Arbeiten zwei Sicherheitseingänge im Zweikanalmodus, wird die Zeitabweichung zwischen der Änderung des Zustands eines der beiden Eingänge bis zur Änderung des Zustands des anderen Eingangs ermittelt. Erfolgt die Änderung des Zustands des anderen Eingangs nicht innerhalb der vorgegebenen Diskrepanzzeit, erkennt der Sicherheitsnetzwerk-Controller NE1A-SCPU01 das Vorliegen eines Fehlers. Die zulässige Verzögerungszeit (Diskrepanzzeit) kann zwischen 0 (ungültig) und 65.530 ms in Schritten von 10 ms eingestellt werden.
Im Einkanalmodus kann keine Einstellung der Diskrepanzzeit erfolgen.

Normales Verhalten bei zwei im Zweikanal-Äquivalenzmodus betriebenen Sicherheitseingängen



Fehlerhaftes Verhalten bei zwei im Zweikanal-Äquivalenzmodus betriebenen Sicherheitseingängen (Diskrepanzfehler)



Hinweis Der Sicherheitsnetzwerk-Controller NE1A bietet Funktionsblöcke mit einer den Zweikanalmodi gleichwertigen Funktionalität. Bei Verwendung eines derartigen Funktionsblocks kann der Sicherheitseingang im Einkanalmodus betrieben werden.

5-2-6 Fehlerbehandlung

Verhalten bei Fehlererkennung

Verhalten im Einkanalmodus

Werden während der Selbstdiagnose Fehler festgestellt, werden die folgenden Aktionen durchgeführt:

- Die E/A-Tags, die den vom Fehler betroffenen Sicherheitseingängen entsprechen, werden deaktiviert.
- Die LED-Anzeigen der vom Fehler betroffenen Sicherheitseingänge leuchten rot.
- Der Fehler wird in das Fehlerprotokoll aufgenommen.
- Der Sicherheitsnetzwerk-Controller NE1A arbeitet weiter.

Verhalten im Zweikanalmodus

Beim Auftreten eines Diskrepanzfehlers werden die folgenden Aktionen durchgeführt:

- Die E/A-Tags, die den beiden vom Fehler betroffenen Sicherheitseingängen entsprechen, werden deaktiviert.
- Die LED-Anzeigen der beiden vom Fehler betroffenen Sicherheitseingänge leuchten rot.
- Die Fehler werden in das Fehlerprotokoll aufgenommen.
- Der Sicherheitsnetzwerk-Controller NE1A arbeitet weiter.

Wird bei einem im Zweikanalmodus betriebenen Sicherheitseingang ein Fehler festgestellt, werden die folgenden Aktionen durchgeführt:

- Die E/A-Tags, die den beiden vom Fehler betroffenen Sicherheitseingängen entsprechen, werden deaktiviert.
- Die LED-Anzeige des vom Fehler betroffenen Sicherheitseingangs leuchtet rot, die LED-Anzeige des zugehörigen anderen Sicherheitseingangs blinkt rot.
- Die Fehler werden in das Fehlerprotokoll aufgenommen.
- Der Sicherheitsnetzwerk-Controller NE1A arbeitet weiter.

Error Latch Time (Parameter)

Mithilfe dieses Parameters kann festgelegt werden, wie lange der Fehlerzustand mindestens gehalten wird, wenn ein Fehler in einem der Sicherheitseingänge festgestellt wird. Auch nach zeitweiliger Behebung der Fehlerursache bleibt der Fehlerzustand für die hier eingestellte Zeitdauer (Fehlerhaltezeit) gehalten. Berücksichtigen Sie bei der Fehlerüberwachung über ein Überwachungssystem den Überwachungsintervall, wenn Sie die Fehlerhaltezeit einstellen.

Diese kann in Schritten von 10 ms zwischen 0 und 65.530 ms eingestellt werden. Die Standardeinstellung beträgt 1.000 ms.

Zurücksetzen von Fehlern

Zum Aufheben des Fehlerzustands nach dem Auftreten eines Fehlers in einem der Sicherheitseingänge müssen sämtliche folgenden Bedingungen erfüllt werden:

- Die Ursache des Fehlers wurde beseitigt.
- Die Fehlerhaltezeit ist abgelaufen.
- Das Eingangssignal muss zu einem inaktiven Status zurückkehren und es darf keine Fehlerbedingung erkannt werden. (z.B. durch Drücken des NOT-AUS-Tasters oder durch Öffnen einer Tür)

5-3 Testausgänge

5-3-1 Test Output Mode (Parameter)

Der Sicherheitsnetzwerk-Controller NE1A-SCPU01(-V1) ist mit vier Testausgängen ausgestattet.

Der Sicherheitsnetzwerk-Controller NE1A-SCPU02 ist mit acht Testausgängen ausgestattet.

Diese können wie in der folgenden Tabelle aufgeführt eingestellt und genutzt werden.

Einstellung	Beschreibung
Not used	Dieser Testausgang wird nicht verwendet.
Standard output	Der Testausgang ist an den Eingang einer Leuchtanzeige oder einer SPS angeschlossen und fungiert als Überwachungsausgang.
Pulse test output	Dieser Testausgang wird gemeinsam mit einem Sicherheitseingang für den Anschluss eines Sicherheitsgeräts mit Kontaktausgang verwendet. Der Testausgang gibt Testimpulse aus, die eine Überwachung der Verbindungen zum Sicherheitsgerät ermöglichen. Die Ausgabe der Testimpulse an den einzelnen Testausgängen erfolgt zeitlich versetzt.
Muting lamp output	Der Testausgang dient zur Ansteuerung einer Muting-Lampe. Ist der Ausgang auf EIN gesetzt, kann eine Unterbrechung der Verbindung zur Muting-Leuchte festgestellt werden. Bei der Ausführung NE1A-SCPU01 kann dieser Modus nur für die Klemme T3 eingestellt werden. Bei der Ausführung NE1A-SCPU02 kann dieser Modus nur für die Klemme T3 oder T7 eingestellt werden.

5-3-2 Fehlerbehandlung

Verhalten bei Fehlererkennung

Werden während der Selbstdiagnose Fehler festgestellt, werden die folgenden Aktionen durchgeführt:

- Die Ausgangsklemmen, an denen Fehler erkannt wurden, werden ohne Eingriff des Anwenderprogramms deaktiviert.
- Der Fehler wird im Fehlerprotokoll gespeichert.
- Der Sicherheitsnetzwerk-Controller NE1A arbeitet weiter.

Error Latch Time (Parameter)

Mithilfe dieses Parameters kann festgelegt werden, wie lange der Fehlerzustand mindestens aktiviert wird, wenn ein Fehler in einem der Sicherheitsausgänge oder Testausgänge festgestellt wird. Auch nach zeitweiliger Behebung der Fehlerursache bleibt der Fehlerzustand für die hier eingestellte Zeitdauer (Fehlerhaltezeit) gehalten. Berücksichtigen Sie bei der Fehlerüberwachung über ein Überwachungssystem den Überwachungsintervall, wenn Sie die Fehlerhaltezeit einstellen. Diese kann in Schritten von 10 ms zwischen 0 und 65.530 ms eingestellt werden. Die Standardeinstellung beträgt 1.000 ms.

Zurücksetzen von Fehlern

Fehler, die an Testausgängen erkannt wurden, werden nach Ablauf der Fehlerhaltezeit automatisch zurückgesetzt. Das Beibehalten von Kurzschlusszuständen kann zu Fehlfunktionen aufgrund zu hoher Temperaturen führen. Beseitigen Sie bei Kurzschlüssen externer Verbraucher umgehend die Ursache.

5-4 Sicherheitsausgänge

5-4-1 Übersicht

Sie Sicherheitsnetzwerk-Controller NE1A-SCPU01(-V1) und NE1A-SCPU02 sind mit acht Sicherheitsausgängen ausgestattet.

Durch Einrichtung und Verdrahtung entsprechend der Art der anzuschließenden externen Geräte oder des zu erreichenden Sicherheitsniveaus kann der Sicherheitsnetzwerk-Controller NE1A flexibel für die verschiedensten Anwendungen eingesetzt werden.

Der Sicherheitsnetzwerk-Controller NE1A kann die folgenden Fehler an den Ausgangssignalleitungen erkennen:

- Kurzschluss mit der Versorgungsspannungsleitung (nur wenn der Ausgang auf AUS geschaltet ist)
- Erdschluss

Bei Verwendung der Testimpulsausgänge können die folgenden Fehler erkannt werden:

- Kurzschluss mit der Versorgungsspannungsleitung (nur wenn der Ausgang auf AUS geschaltet ist)
- Erdschluss
- Querschluss zwischen Ausgangssignalleitungen

5-4-2 Output Channel Mode (Parameter)

Je nach angeschlossenem externem Gerät muss der Parameter „Output Channel Mode“ (Betriebsart für die lokalen Sicherheitsausgänge) entsprechend gesetzt werden. Details zu den Modi finden Sie in der nachstehenden Tabelle.

Einstellung	Beschreibung
Not used	An diesen Ausgang ist kein externes Gerät angeschlossen.
Safety	Ist der Ausgang auf EIN geschaltet, werden keine Testimpulse ausgegeben. Kurzschlüsse zwischen der Ausgangssignalleitung und der Versorgungsspannungsleitung (wenn der Ausgang auf AUS geschaltet ist) und Erdschlüsse werden erkannt.
Safety pulse output	Ist der Ausgang auf EIN geschaltet, werden Testimpulse ausgegeben. Auf diese Weise können Kurzschlüsse mit der Versorgungsspannungsleitung (unabhängig vom Einschaltzustand des Ausgang), Erdschlüsse sowie Querschlüsse zwischen Ausgangssignalleitungen erkannt werden.

WICHTIG Bei der Einstellung „Safety pulse output“ (Sicherheitsimpulsausgang) wird zur Diagnose des Ausgangsschaltkreises ein AUS-Impulssignal (Impulsdauer: 580 μs) ausgegeben, wenn der Sicherheitsausgang auf EIN gesetzt wird. Verifizieren Sie, dass die Eingangsansprechzeit des an den Sicherheitsnetzwerk-Controller NE1A angeschlossenen Steuergeräts lang genug ist, damit dieser Ausgangsimpuls zu keinen Fehlfunktionen führt.

5-4-3 Dual Channel Mode (Parameter)

Die lokalen Sicherheitsausgänge des Sicherheitsnetzwerk-Controllers NE1A können paarweise im Zweikanalmodus betrieben werden. Dieser Modus bietet die folgenden Möglichkeiten:

- Entsprechen die Einschaltzustände der beiden Ausgänge einander nicht (z. B. aufgrund eines Fehlers im Anwenderprogramm), wird das Vorliegen eines Fehlers erkannt.

- Wird ein Fehler in einem der beiden Ausgangsschaltkreise festgestellt, werden beide Ausgänge deaktiviert.

Einstellung	Beschreibung
Single Channel	Der Eingang wird als unabhängiger Sicherheitsausgang verwendet.
Dual Channel	Betrieb des Sicherheitsausgangs in Verbindung mit einem zweiten Sicherheitsausgang im Zweikanalmodus. Der Ausgang wird nur dann auf EIN geschaltet, wenn die E/A-Tags beider Sicherheitsausgänge auf EIN geschaltet sind, d. h. kein Diskrepanzfehler vorliegt.

Abbildung des Zustands der E/A-Tags an den Sicherheitsausgangsklemmen

Die nachstehenden Tabellen erläutern, wie der Status der E/A-Tags der Sicherheitsausgänge im Ein- und Zweikanalmodus an den entsprechenden Sicherheitsausgangsklemmen abgebildet wird.

Modus	E/A-Tag	Sicherheitsausgangsklemme	Bedeutung
	OUT (x)	OUT (x)	
Single Channel	0	0	AUS
	1	1	EIN

X: 0 bis 7

Einstellung	E/A-Tag		Sicherheitsausgangsklemme		Bedeutung
	IN (n)	IN (n+1)	OUT (n)	OUT (n+1)	
Dual Channel	0	0	0 (AUS)	0 (AUS)	AUS
	0	1	0 (AUS)	0 (AUS)	Diskrepanzfehler
	1	0	0 (AUS)	0 (AUS)	Diskrepanzfehler
	1	1	1 (EIN)	1 (EIN)	EIN

n = Gerade Zahl

5-4-4 Fehlerbehandlung

Verhalten bei Fehlererkennung

Verhalten im Einkanalmodus

Werden während der Selbstdiagnose Fehler festgestellt, werden die folgenden Aktionen durchgeführt:

- Unabhängig vom Zustand des durch das Anwenderprogramm gesetzten E/A-Tags wird der Ausgang auf AUS geschaltet.
- Die LED-Anzeige des vom Fehler betroffenen Sicherheitsausgangs leuchtet rot.
- Der Fehler wird in das Fehlerprotokoll aufgenommen.
- Der Sicherheitsnetzwerk-Controller NE1A arbeitet weiter.

Verhalten im Zweikanalmodus

Wird bei einem im Zweikanalmodus betriebenen Sicherheitsausgang ein Fehler festgestellt, werden die folgenden Aktionen durchgeführt:

- Unabhängig vom Zustand der durch das Anwenderprogramm gesetzten E/A-Tags werden die beiden gemeinsam im Zweikanalmodus betriebenen Ausgänge auf AUS geschaltet.

- Die LED-Anzeige des vom Fehler betroffenen Sicherheitsausgangs leuchtet rot, die LED-Anzeige des zugehörigen anderen Sicherheitsausgangs blinkt rot.
- Der Fehler wird in das Fehlerprotokoll aufgenommen.
- Der Sicherheitsnetzwerk-Controller NE1A arbeitet weiter.

Beim Auftreten eines Diskrepanzfehlers (Abweichungen zwischen den E/A-Tags der beiden Sicherheitsausgänge) werden die folgenden Aktionen durchgeführt:

- Unabhängig vom Zustand der durch das Anwenderprogramm gesetzten E/A-Tags werden die beiden gemeinsam im Zweikanalmodus betriebenen Ausgänge auf AUS geschaltet.
- Die LED-Anzeigen der beiden Sicherheitsausgänge leuchten rot.
- Der Fehler wird in das Fehlerprotokoll aufgenommen.
- Der Sicherheitsnetzwerk-Controller NE1A arbeitet weiter.

Error Latch Time (Parameter)

Mithilfe dieses Parameters kann festgelegt werden, wie lange der Fehlerzustand mindestens aktiviert wird, wenn ein Fehler in einem der Sicherheitsausgänge festgestellt wird. Auch nach zeitweiliger Behebung der Fehlerursache bleibt der Fehlerzustand für die hier eingestellte Zeitdauer (Fehlerhaltezeit) gehalten. Berücksichtigen Sie bei der Fehlerüberwachung über ein Überwachungssystem den Überwachungsintervall, wenn Sie die Fehlerhaltezeit einstellen.

Diese kann in Schritten von 10 ms zwischen 0 und 65.530 ms eingestellt werden. Die Standardeinstellung beträgt 1.000 ms.

Zurücksetzen von Fehlern

Zum Aufheben des Fehlerzustands nach dem Auftreten eines Fehlers in einem der Sicherheitsausgänge müssen sämtliche folgenden Bedingungen erfüllt werden:

- Die Ursache des Fehlers wurde beseitigt.
- Die Fehlerhaltezeit ist abgelaufen.
- Die E/A-Tags, die den vom Fehler betroffenen Sicherheitsausgängen entsprechen, wurden deaktiviert.

Hinweis Bei Verwendung des Zweikanalmodus für die Realisierung einer redundanten Schaltung wird beim Auftreten eines Fehlers in einem der Ausgänge der andere Ausgang automatisch auf AUS geschaltet, ohne dass hierfür entsprechende Vorkehrungen im Anwenderprogramm getroffen werden müssen. Erfolgt die Realisierung einer redundanten Schaltung mittels zwei im Einkanalmodus betriebenen Ausgängen, muss die Erkennung eines Diskrepanzfehlers durch entsprechende Schritte im Anwenderprogramm (beispielsweise durch Verwendung des Funktionsblocks „External Device Monitoring“) erfolgen.

ABSCHNITT 6
Programmierung

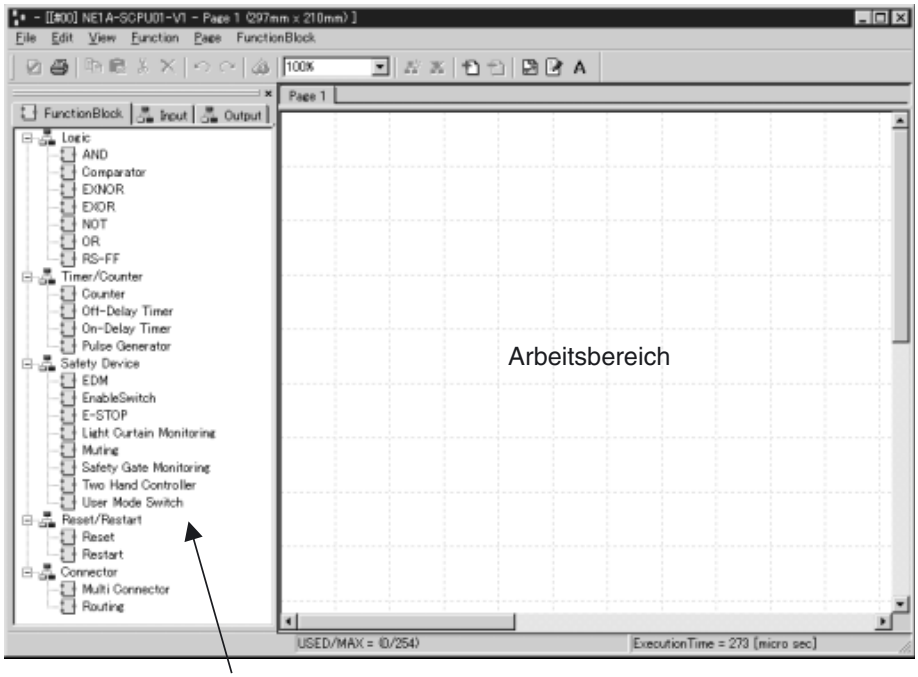
6-1 Übersicht über die Programmierung 108
6-1-1 Übersicht 108
6-1-2 Grundlagen der Programmierung 108
6-1-3 Programmkapazität 110
6-2 Funktionsblöcke – Übersicht 111
6-2-1 Unterstützte Funktionsblöcke 111
6-3 Parametrieren von Funktionsblöcken 112
6-3-1 Festlegen von Funktionsblockparametern 112
6-3-2 E/A-Einstellungen 115
6-4 Befehlsreferenz: Logikfunktionen 117
6-4-1 Logikfunktion: NOT 117
6-4-2 Logikfunktion: AND 117
6-4-3 Logikfunktion: OR 121
6-4-4 Logikfunktion: XOR 123
6-4-5 Logikfunktion: XNOR 124
6-4-6 Logikfunktion: RS-FF (Reset Set Flip-Flop) 124
6-4-7 Logikfunktion: Komparator 126
6-5 Befehlsreferenz: Funktionsblöcke 129
6-5-1 Funktionsblock: Rücksetzung 129
6-5-2 Funktionsblock: Restart 132
6-5-3 Funktionsblock: NOT-AUS-Taster-Überwachung 134
6-5-4 Funktionsblock: Lichtgitter-Überwachung 137
6-5-5 Funktionsblock: Sicherheitstür-Überwachung 139
6-5-6 Funktionsblock: Zweihandsteuerung 145
6-5-7 Funktionsblock: Ausschaltverzögerung 148
6-5-8 Funktionsblock: Einschaltverzögerung 149
6-5-9 Funktionsblock: Betriebsartenwahlschalter 150
6-5-10 Funktionsblock: Externe Relaisüberwachung 152
6-5-11 Logikfunktion: Routing 153
6-5-12 Funktionsblock: Muting 154
6-5-13 Funktionsblock: Zustimmschalterüberwachung 170
6-5-14 Funktionsblock: Impulsgeber 172
6-5-15 Funktionsblock: Zähler 173
6-5-16 Logikfunktion: Multi Connector 175

6-1 Übersicht über die Programmierung

6-1-1 Übersicht

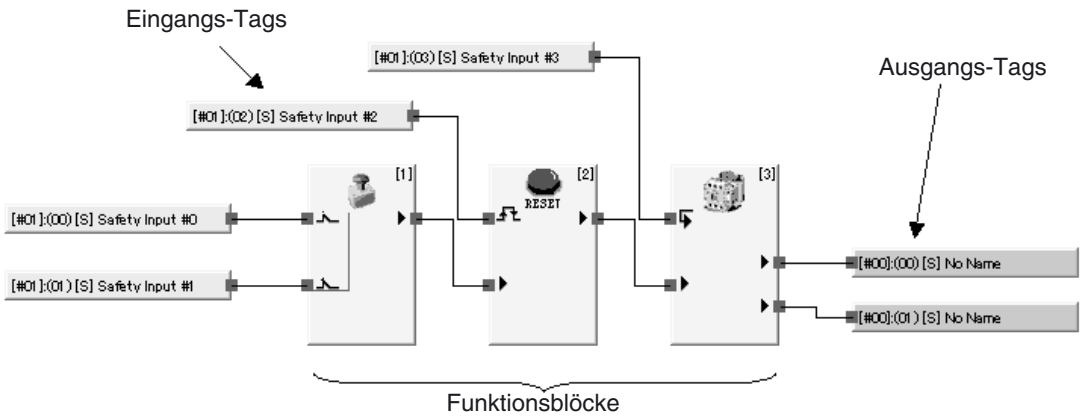
Die Programmierung des Sicherheitsnetzwerk-Controllers NE1A erfolgt durch den Aufruf eines Logik-Editors des Netzwerkkonfigurators. Wie aus der nachstehenden Abbildung ersichtlich umfasst dieser Logik-Editor eine Funktionsliste mit Funktionsblöcken, E/A-Tags und anderen Programmierelementen sowie einen Arbeitsbereich, in dem die eigentliche Programmierung erfolgt.

Die Programmierung erfolgt unter Verwendung der in der Funktionsliste registrierten Funktionsblöcke, E/A-Tags und anderen Programmierelemente.



6-1-2 Grundlagen der Programmierung

Bei der Erstellung von Programmen werden Logikfunktionen und Funktionsblöcke (Befehle) mit Eingangs-Tags (Signalquellen) und Ausgangs-Tags (Signalzielen) durch Verbindungslinien verknüpft.

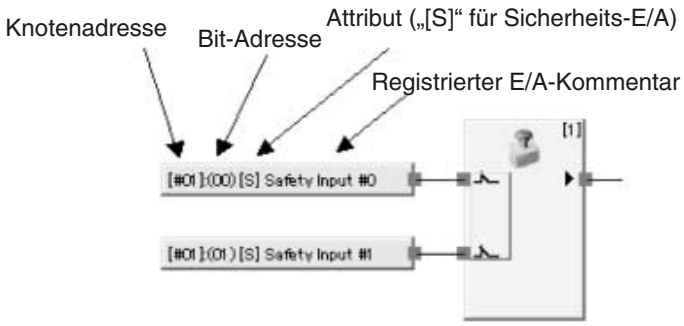


■ **Eingangs-Tags**

Eingangs-Tags entsprechen dem Status von Eingängen der folgenden E/A-Bereiche:

- Eingangsbereich lokaler Klemmen des Sicherheitsnetzwerk-Controller NE1A
- Eingangsbereich von als Kommunikationspartnern registrierten Sicherheits-Slaves
- Der den Daten des Sicherheits-Masters entsprechende E/A-Bereich
- Der den Daten des Standard-Masters entsprechende E/A-Bereich

Die im Logik-Editor verwendeten Eingangs-Tags enthalten die folgenden Informationen:



Bei Controllern ab Geräteversion 1.0 werden Daten in den folgenden E/A-Bereichen abgebildet.

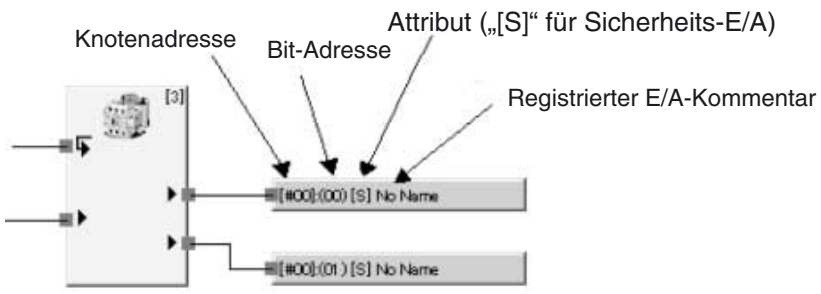
- Status der lokalen Eingänge
- Status der lokalen Ausgänge
- Allgemeiner Gerätestatus
- Status der Testausgänge
- Muting-Lampen-Status

■ **Ausgangs-Tags**

Ausgangs-Tags entsprechen dem Status von Ausgängen der folgenden E/A-Bereiche:

- Ausgangsbereich lokaler Klemmen des Sicherheitsnetzwerk-Controller NE1A
- Ausgangsbereich von als Kommunikationspartnern registrierten Sicherheits-Slaves
- Der den Daten des Sicherheits-Masters entsprechende E/A-Bereich
- Der den Daten des Standard-Masters entsprechende E/A-Bereich

Die im Logik-Editor verwendeten Ausgangs-Tags enthalten die folgenden Informationen:



⚠ VORSICHT
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, Achten Sie darauf, dass die in der Sicherheitssteuerung eingesetzten Sicherheitssignale die anwendbaren Normen und Bestimmungen erfüllen. Verwenden Sie nur Sicherheitssignale als Eingänge für Funktionsblöcke. Die Sicherstellung ordnungsgemäßer Signalquellen für diese Funktionsblöcke und die Einhaltung der anwendbaren Sicherheitsnormen und -bestimmungen durch das Gesamtkonzept der Sicherheitssteuerung liegt in der alleinigen Verantwortung des Anwenders.
Beim Ausfall der erforderlichen Sicherheitsfunktionen besteht die Gefahr von schweren Verletzungen. Bei der Implementierung von Sicherheitsfunktionen müssen Sie sicherstellen, dass die Steuerungsstrategie und die eingesetzten Risikovermeidungstechniken den lokalen, regionalen und nationalen Richtlinien entsprechen. Ziehen Sie für die Bestimmung der für Ihre Anwendung zutreffenden Anforderungen diese Bestimmungen und Industriestandards zu Rate.

6-1-3 Programmkapazität

Die nachstehende Tabelle informiert über die maximale Größe von Anwenderprogrammen für den Sicherheitsnetzwerk-Controller NE1A.

Modell	Gesamtanzahl von Logikfunktionen und Funktionsblöcken
NE1A-SCPU01	128
NE1A-SCPU01-V1	254
NE1A-SCPU02	254

6-2 Funktionsblöcke – Übersicht

Die Logikprogrammierung des Sicherheitsnetzwerk-Controllers NE1A erfolgt unter Verwendung von Funktionsblöcken. Die Verwendung der in diesem Abschnitt beschriebenen Funktionsblöcke ermöglicht die Erstellung der verschiedensten, den Sicherheitsnormen genügenden Sicherheitsanwendungen.

6-2-1 Unterstützte Funktionsblöcke

Aus der nachstehenden Tabelle geht hervor, welche Logik-Funktionen und Funktionsblöcke vom Sicherheitsnetwerk-Controller NE1A der jeweiligen Geräteversion unterstützt werden.

Logikfunktionen

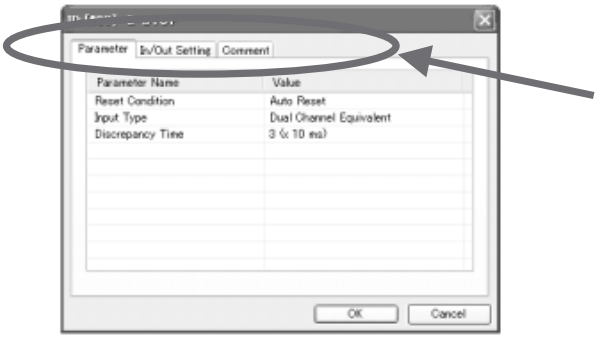
Eintrag	Bezeichnung in der Funktionsliste	Kompatible Geräteversionen
NOT	NOT	Alle
AND	AND	Alle
OR	OR	Alle
XOR	EXOR	Alle
XNOR	EXNOR	Alle
RS Flip-flop	RS-FF	Ab Geräteversion 1.0
Komparator	Comparator	Ab Geräteversion 1.0

Funktionsblöcke

Eintrag	Bezeichnung in der Funktionsliste	Kompatible Geräteversionen
Rücksetzung	Reset	Alle
Neustart	Restart	Alle
NOT-AUS-Taster-Überwachung	E-STOP	Alle
Lichtgitter-Überwachung	Light Curtain Monitoring	Alle
Sicherheitstür-Überwachung	Safety Gate Monitoring	Alle
Zweihandsteuerung	Two Hand Controller	Alle
Ausschaltverzögerung	Off-Delay Timer	Alle
Einschaltverzögerung	On-Delay Timer	Alle
Betriebsartenwahlschalter	User Mode Switch	Alle
Externe Relaisüberwachung	EDM	Alle
Routing	Routing	Alle
Muting	Muting	Ab Geräteversion 1.0
Zustimmschalter	EnableSwitch	Ab Geräteversion 1.0
Impulsgeber	Pulse Generator	Ab Geräteversion 1.0
Zähler	Counter	Ab Geräteversion 1.0
Multiverbinder	Multi Connector	Ab Geräteversion 1.0

6-3 Parametrieren von Funktionsblöcken

Durch Parametrierung von Funktionsblöcken können Sie Parameter festlegen sowie zusätzliche E/A-Punkte und erläuternde Kommentare hinzufügen.



Registerkarten:
Funktionsblockparameter
Ein-/Ausgangseinstellungen
Anmerkungen

6-3-1 Festlegen von Funktionsblockparametern

Zur Anpassung an die jeweilige Anwendung können die folgenden Funktionsblockparameter festgelegt werden. Die konkret festzulegenden Parameter variieren von Funktionsblock zu Funktionsblock.

- Input type
- Diskrepanzzeit
- Synchronisationszeit
- Funktionstest

Eingangsarteinstellungen

- Single Channel
- Dual Channel Equivalent
- Dual Channel Complementary
- Dual Channel Equivalent (2 Pairs)
- Dual Channel Complementary (2 Pairs)

Die nachstehenden Wahrheitstabellen erläutern das Verhalten des Sicherheitsnetzwerk-Controllers NE1A bei den genannten Eingangsarten. In diesen Tabellen steht 0 für AUS und 1 für EIN.

Einstellung: Single Channel

Eingang 1 (Öffner)	Output Enable
0	0
1	1

Einstellung: Dual Channel Equivalent

Eingang 1 (Öffner)	Eingang 2 (Öffner)	Output Enable
0	0	0
0	1	0
1	0	0
1	1	1

Einstellung: Dual Channel Complementary

Eingang 1 (Öffner)	Eingang 2 (Schließer)	Ausgang „Output Enable“
0	0	0
0	1	0
1	0	1
1	1	0

Einstellung: Dual Channel Equivalent (2 Paare)

Eingang 1 (Öffner)	Eingang 2 (Öffner)	Eingang 3 (Öffner)	Eingang 4 (Öffner)	Output Enable
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	0
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	1

Einstellung: Dual Channel Complementary (2 Pairs)

Eingang 1 (Öffner)	Eingang 2 (Schließer)	Eingang 3 (Öffner)	Eingang 4 (Schließer)	Output Enable
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	1
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

Diskrepanzzeit

Bei Verwendung einer der Eingangsarten „Dual Channel Equivalent“ oder „Dual Channel Complementary“ kann die Diskrepanzzeit (die zeitliche Abweichung zwischen den Zustandsänderungen der beiden Eingänge) ausgewertet werden.

Dabei wird die Zeit zwischen der Änderung des Zustands eines der beiden im Zweikanalmodus betriebenen Eingänge bis zur Änderung des Zustands des anderen Eingangs überwacht. Erfolgt diese Zustandsänderung nicht vor Ablauf der eingestellten Diskrepanzzeit, tritt ein Fehler auf und der Ausgang „Output Enable“ des Funktionsblocks wird nicht auf EIN gesetzt.

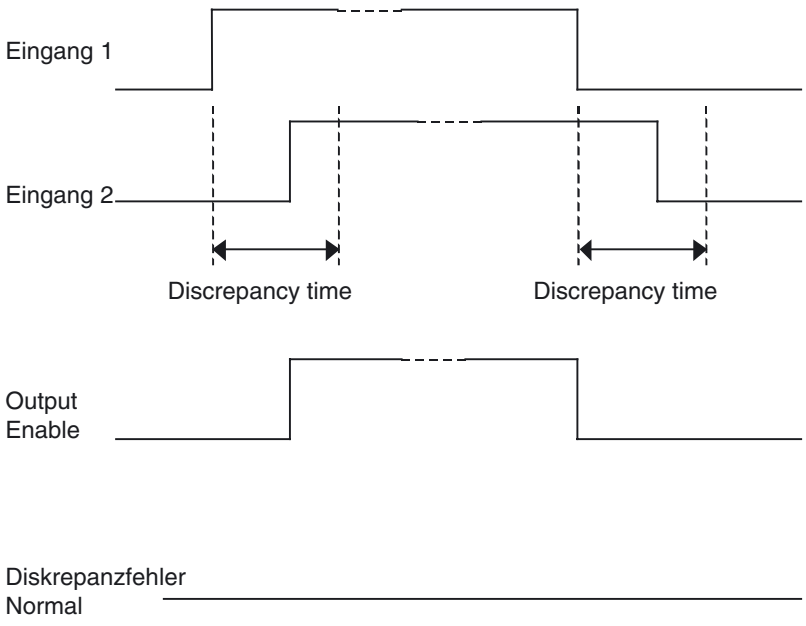
Zweikanalmodus	Eingangssignale		Eingangssignalstatus
	Eingang 1	Eingang 2	
Dual Channel Equivalent • Eingang 1: Öffner • Eingang 2: Öffner	0	0	Inaktiv
	0	1	abweichend
	1	0	abweichend
	1	1	Aktiv
Dual Channel Complementary • Eingang 1: Öffner • Eingang 2: Schließer	0	0	abweichend
	0	1	Inaktiv
	1	0	Aktiv
	1	1	abweichend

Die Zweikanalmodi können zur Feststellung von Fehlern in Sicherheitsgeräten und deren Verdrahtung eingesetzt werden.

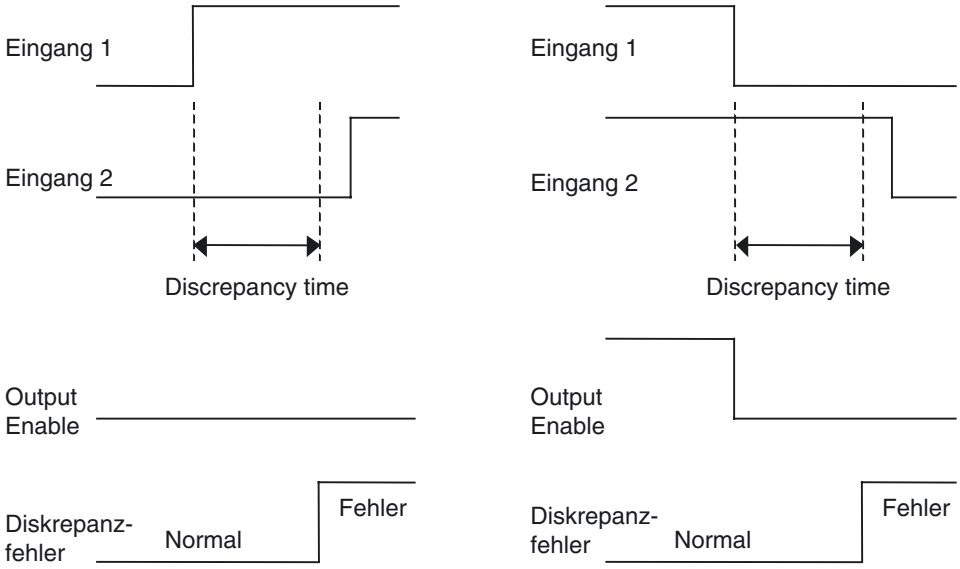
Die Zeit zwischen Eingangsänderungen wird nicht überwacht, wenn die Diskrepanzzeit auf „0“ gesetzt wird.

Die Überwachung der Diskrepanzzeit erfolgt sowohl beim Übergang von EIN nach AUS als auch beim Übergang von AUS nach EIN.

■ **Normales Verhalten bei der Einstellung „Dual Channel Equivalent“**



■ **Verhalten im Fehlerfall bei der Einstellung „Dual Channel Equivalent“**



Synchronisationszeit

Bei Verwendung einer der Eingangsarten „Dual Channel Equivalent (2 Paare)“ oder „Dual Channel Complementary (2 Paare)“ kann die Synchronisationszeit (die zeitliche Abweichung zwischen den Zustandsänderungen der beiden Eingangspaare) ausgewertet werden.

Dabei wird die Zeit zwischen der Änderung des Zustands eines der beiden Eingangspaare bis zur Änderung des Zustands des anderen Eingangspaars überwacht. Erfolgt diese Zustandsänderung nicht vor Ablauf der eingestellten Synchronisationszeit, tritt ein Fehler auf und der Ausgang „Output Enable“ des Funktionsblocks wird nicht auf EIN gesetzt. Die Zeit zwischen Änderungen in den Eingangspaaren wird nicht überwacht, wenn die Synchronisationszeit auf „0“ gesetzt wird.

Funktionstests

Der Funktionsblock für die Überwachung von Sicherheitstüren („Safety Gate Monitoring“) unterstützt die Verwendung von Funktionstests.

Ist die Funktionstest-Option beim Start des Sicherheitsnetzwerk-Controllers NE1A aktiviert, muss ein Test der Sicherheitstür durchgeführt werden, wenn das Funktionstestanforderungssignal von der Maschine gegeben wird.

6-3-2 E/A-Einstellungen

Ein- und Ausgangsgrößeneinstellungen

Die Anzahl der Ein- und Ausgänge für Logik-Funktionen kann erhöht werden.

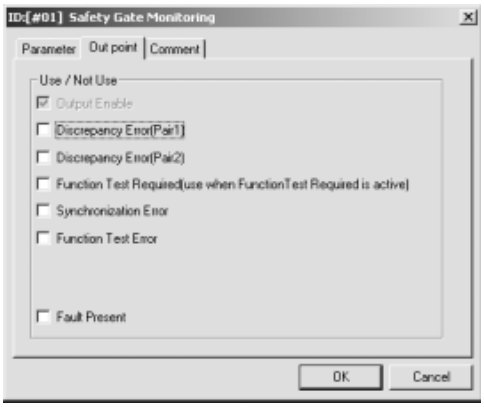
Ausgangspunkte-Einstellung

Optionale Ausgänge von Funktionsblöcken können aktiviert werden.

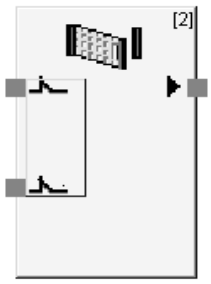
Einstellung „Use Fault Present“

Fault Present ist ein von manchen Funktionsblöcken unterstütztes diagnostisches Statusbit. Zur Verwendung dieses Statusbits muss das entsprechende Kontrollkästchen auf der Registerkarte „In/Out Setting“ oder „Out Point“ des Eigenschaftendialogfelds des jeweiligen Funktionsblocks aktiviert werden. Ist dieses Kontrollkästchen *Fault Present* aktiviert, verfügt der Funktionsblock über einen zusätzlichen Ausgang „Fault Present“ (Fehlerzustand).

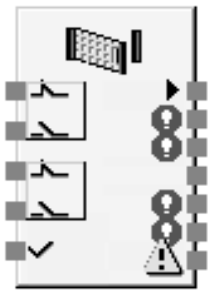
Beispiel: Funktionsblock für die Sicherheitstür-Überwachung (SGATE)



Registerkarte „Out Point“ des Eigenschaftendialogfelds des Funktionsblocks für die Sicherheitstür-Überwachung (SGATE).



Funktionsblock für die Sicherheitstür-Überwachung (SGATE) mit Standard-Eingängen und -Ausgängen

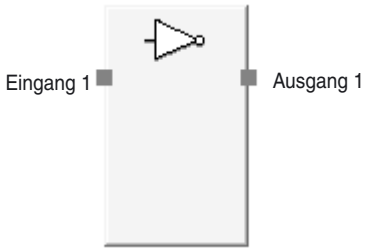


Funktionsblock für die Sicherheitstür-Überwachung (SGATE) mit maximaler Eingangszahl und sämtlichen optionalen Ausgängen

6-4 Befehlsreferenz: Logikfunktionen

6-4-1 Logikfunktion: NOT

Diagramm



Allgemeine Beschreibung

Der Ausgang entspricht dem invertierten Eingang.

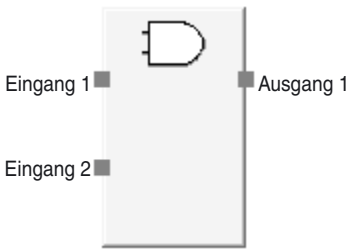
Wahrheitstabelle

Eingang 1	Ausgang 1
0	1
1	0

0: AUS, 1: EIN

6-4-2 Logikfunktion: AND

Diagramm



Standardbelegung (Ein- und Ausgänge)

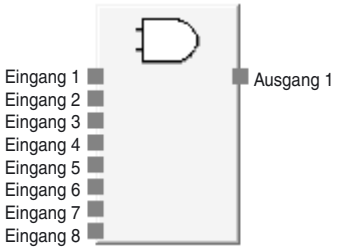
Allgemeine Beschreibung

Der Ausgang entspricht der logischen UND-Verknüpfung der Eingänge. Diese Logikfunktion kann bis zu acht Eingänge besitzen.

Optionale Eingangseinstellungen

Die Anzahl der Eingänge kann auf der Registerkarte „In/Out Setting“ des Eigenschaftendialogfelds der Logikfunktion auf einen Wert zwischen 1 und 8 eingestellt werden.

Einstellung	Einstellbereich	Standardeinstellung
Number of Inputs	1 bis 8	2



Logikfunktion AND mit der maximal möglichen Zahl von Eingängen

Wahrheitstabellen

Wahrheitstabelle für die Logikfunktion AND mit einem Eingang

Eingang 1	Ausgang 1
0	0
1	1

0: AUS, 1: EIN

Wahrheitstabelle für die Logikfunktion AND mit zwei Eingängen

Eingang 1	Eingang 2	Ausgang 1
0	x	0
x	0	0
1	1	1

0: AUS, 1: EIN, x: wahlweise EIN oder AUS

Wahrheitstabelle für die Logikfunktion AND mit drei Eingängen

Eingang 1	Eingang 2	Eingang 3	Ausgang 1
0	x	x	0
x	0	x	0
x	x		

0: AUS, 1: EIN, x: wahlweise EIN oder AUS

Wahrheitstabelle für die Logikfunktion AND mit vier Eingängen

Eingang 1	Eingang 2	Eingang 3	Eingang 4	Ausgang 1
0	x	x	x	0
x	0	x	x	0
x	x	0	x	0
x	x	x	0	0
1	1	1	1	1

0: AUS, 1: EIN, x: wahlweise EIN oder AUS

Wahrheitstabelle für die Logikfunktion AND mit fünf Eingängen

Eingang 1	Eingang 2	Eingang 3	Eingang 4	Eingang 5	Ausgang 1
0	x	x	x	x	0
x	0	x	x	x	0
x	x	0	x	x	0
x	x	x	0	x	0
x	x	x	x	0	0
1	1	1	1	1	1

0: AUS, 1: EIN, x: wahlweise EIN oder AUS

Wahrheitstabelle für die Logikfunktion AND mit sechs Eingängen

Eingang 1	Eingang 2	Eingang 3	Eingang 4	Eingang 5	Eingang 6	Ausgang 1
0	x	x	x	x	x	0
x	0	x	x	x	x	0
x	x	0	x	x	x	0
x	x	x	0	x	x	0
x	x	x	x	0	x	0
x	x	x	x	x	0	0
1	1	1	1	1	1	1

0: AUS, 1: EIN, x: wahlweise EIN oder AUS

Wahrheitstabelle für die Logikfunktion AND mit sieben Eingängen

Eingang 1	Eingang 2	Eingang 3	Eingang 4	Eingang 5	Eingang 6	Eingang 7	Ausgang 1
0	x	x	x	x	x	x	0
x	0	x	x	x	x	x	0
x	x	0	x	x	x	x	0
x	x	x	0	x	x	x	0
x	x	x	x	0	x	x	0
x	x	x	x	x	0	x	0
x	x	x	x	x	x	0	0
1	1	1	1	1	1	1	1

0: AUS, 1: EIN, x: wahlweise EIN oder AUS

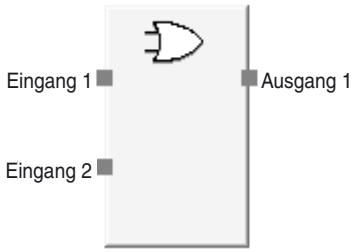
Wahrheitstabelle für die Logikfunktion AND mit acht Eingängen

Eingang 1	Eingang 2	Eingang 3	Eingang 4	Eingang 5	Eingang 6	Eingang 7	Eingang 8	Ausgang 1
0	x	x	x	x	x	x	x	0
x	0	x	x	x	x	x	x	0
x	x	0	x	x	x	x	x	0
x	x	x	0	x	x	x	x	0
x	x	x	x	0	x	x	x	0
x	x	x	x	x	0	x	x	0
x	x	x	x	x	x	0	x	0
x	x	x	x	x	x	x	0	0
1	1	1	1	1	1	1	1	1

0: AUS, 1: EIN, x: wahlweise EIN oder AUS

6-4-3 Logikfunktion: OR

Diagramm



Standardbelegung (Ein- und Ausgänge)

Allgemeine Beschreibung

Der Ausgang entspricht der logischen ODER-Verknüpfung der Eingänge. Diese Logikfunktion kann bis zu acht Eingänge besitzen.

Optionale Eingangseinstellungen

Die Anzahl der Eingänge kann auf der Registerkarte „In/Out Setting“ des Eigenschaftendialogfelds der Logikfunktion auf einen Wert zwischen 1 und 8 eingestellt werden.

Einstellung	Einstellbereich	Standardeinstellung
Number of Inputs	1 bis 8	2

Logikfunktion OR mit der maximal möglichen Zahl von Eingängen

Wahrheitstabelle

Wahrheitstabelle für die Logikfunktion OR mit einem Eingang

Eingang 1	Ausgang 1
0	0
1	1

0: AUS, 1: EIN

Wahrheitstabelle für die Logikfunktion OR mit zwei Eingängen

Eingang 1	Eingang 2	Ausgang 1
0	0	0
1	x	1
x	1	1

0: AUS, 1: EIN, x: wahlweise EIN oder AUS

Wahrheitstabelle für die Logikfunktion OR mit drei Eingängen

Eingang 1	Eingang 2	Eingang 3	Ausgang 1
0	0	0	0
1	x	x	1
x	1	x	1
x	x	1	1

0: AUS, 1: EIN, x: wahlweise EIN oder AUS

Wahrheitstabelle für die Logikfunktion OR mit vier Eingängen

Eingang 1	Eingang 2	Eingang 3	Eingang 4	Ausgang 1
0	0	0	0	0
1	x	x	x	1
x	1	x	x	1
x	x	1	x	1
x	x	x	1	1

0: AUS, 1: EIN, x: wahlweise EIN oder AUS

Wahrheitstabelle für die Logikfunktion OR mit fünf Eingängen

Eingang 1	Eingang 2	Eingang 3	Eingang 4	Eingang 5	Ausgang 1
0	0	0	0	0	0
1	x	x	x	x	1
x	1	x	x	x	1
x	x	1	x	x	1
x	x	x	1	x	1
x	x	x	x	1	1

0: AUS, 1: EIN, x: wahlweise EIN oder AUS

Wahrheitstabelle für die Logikfunktion OR mit sechs Eingängen

Eingang 1	Eingang 2	Eingang 3	Eingang 4	Eingang 5	Eingang 6	Ausgang 1
0	0	0	0	0	0	0
1	x	x	x	x	x	1
x	1	x	x	x	x	1
x	x	1	x	x	x	1
x	x	x	1	x	x	1
x	x	x	x	1	x	1
x	x	x	x	x	1	1

0: AUS, 1: EIN, x: wahlweise EIN oder AUS

Wahrheitstabelle für die Logikfunktion OR mit sieben Eingängen

Eingang 1	Eingang 2	Eingang 3	Eingang 4	Eingang 5	Eingang 6	Eingang 7	Ausgang 1
0	0	0	0	0	0	0	0
1	x	x	x	x	x	x	1
x	1	x	x	x	x	x	1
x	x	1	x	x	x	x	1
x	x	x	1	x	x	x	1
x	x	x	x	1	x	x	1
x	x	x	x	x	1	x	1
x	x	x	x	x	x	1	1

0: AUS, 1: EIN, x: wahlweise EIN oder AUS

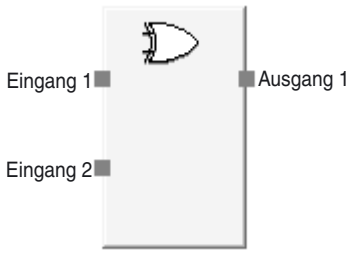
Wahrheitstabelle für die Logikfunktion OR mit acht Eingängen

Eingang 1	Eingang 2	Eingang 3	Eingang 4	Eingang 5	Eingang 6	Eingang 7	Eingang 8	Ausgang 1
0	0	0	0	0	0	0	0	0
1	x	x	x	x	x	x	x	1
x	1	x	x	x	x	x	x	1
x	x	1	x	x	x	x	x	1
x	x	x	1	x	x	x	x	1
x	x	x	x	1	x	x	x	1
x	x	x	x	x	1	x	x	1
x	x	x	x	x	x	1	x	1
x	x	x	x	x	x	x	1	1

0: AUS, 1: EIN, x: wahlweise EIN oder AUS

6-4-4 Logikfunktion: XOR

Diagramm



Allgemeine Beschreibung

Der Ausgang entspricht der logischen Exklusiv-ODER-Verknüpfung (XOR) der Eingänge.

Wahrheitstabellen

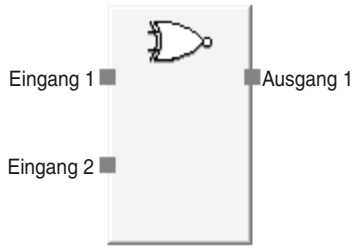
Wahrheitstabelle für die Logikfunktion XOR

Eingang 1	Eingang 2	Ausgang 1
0	0	0
0	1	1
1	0	1
1	1	0

0: AUS, 1: EIN

6-4-5 Logikfunktion: XNOR

Diagramm



Allgemeine Beschreibung

Der Ausgang entspricht der invertierten logischen Exklusiv-ODER-Verknüpfung (XNOR) der Eingänge.

Wahrheitstabellen

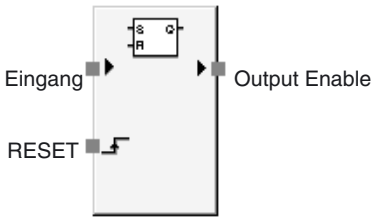
Wahrheitstabelle für die Logikfunktion XNOR

Eingang 1	Eingang 2	Ausgang 1
0	0	1
0	1	0
1	0	0
1	1	1

0: AUS, 1: EIN

6-4-6 Logikfunktion: RS-FF (Reset Set Flip-Flop)

Diagramm



Standardbelegung (Ein- und Ausgänge)

Allgemeine Beschreibung

Diese Funktion steht nur beim Sicherheitsnetzwerk-Controller NE1A ab Geräteversion 1.0 zur Verfügung.

Wenn die Eingangsbedingung für den RS-FF Funktionsblock aktiviert wird (EIN), wird dieser EIN-Status im Funktionsblock gehalten und der EIN-Ausgang wird am Signal „Output Enable“ gehalten.

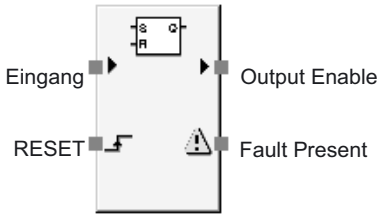
Der EIN-Status wird im Funktionsblock gehalten, sodass das Signal „Output Enable“ auch dann aktiviert bleibt (EIN), wenn der Eingangszustand von EIN nach AUS wechselt.

Das im Funktionsblock gehaltene Signal wird deaktiviert (AUS), wenn die RESET-Bedingung des Funktionsblocks aktiviert wird (EIN).

Einstellung „Use Fault Present“

Bei der Programmierung kann auch der Ausgang „Fault Present“ genutzt werden.

Damit dieser optionale Ausgang im Logik-Editor angezeigt wird, muss das Kontrollkästchen „Fault Present“ auf der Registerkarte „Out Point“ des Eigenschaftendialogfelds des Funktionsblocks aktiviert werden.

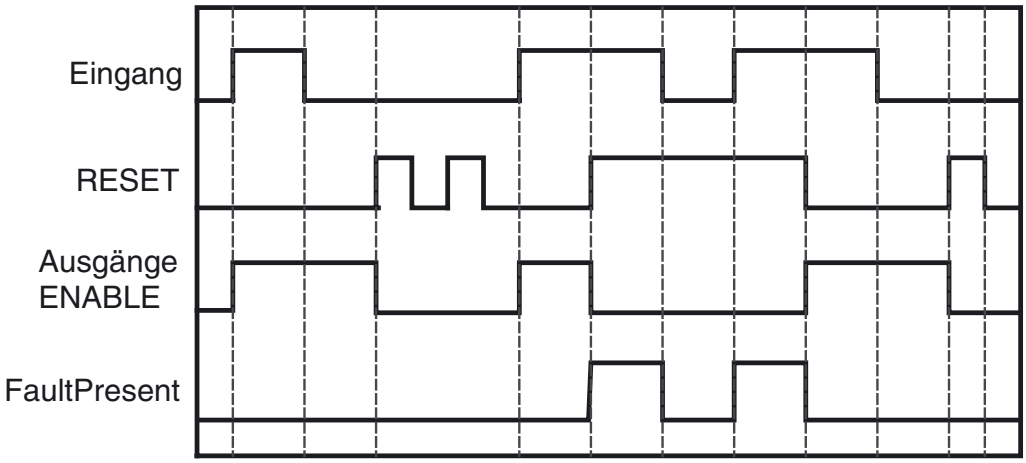


Maximale Anzahl E/A-Punkte für einen RS-FF Funktionsblock

Fehlerbehandlung und Zurücksetzen des Fehlerzustands

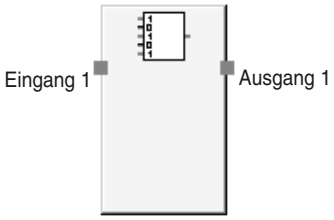
Fehlerzustand	Verhalten bei Fehlererkennung		Zurücksetzen des Fehlerzustands
	Output Enable	Fault Present	
Eingang und RESET sind gleichzeitig aktiv.	AUS (Sicherheits-zustand)	EIN	Eines der Signale deaktivieren.

Zeitdiagramm



6-4-7 Logikfunktion: Komparator

Diagramm



Standardbelegung (Ein- und Ausgänge)

Allgemeine Beschreibung

Diese Funktion steht nur beim Sicherheitsnetzwerk-Controller NE1A ab Geräteversion 1.0 zur Verfügung.

Der Komparator vergleicht die spezifizierten Eingangssignale (bis zu 8 Eingänge) mit dem in der Konfiguration festgelegten Vergleichswert und aktiviert das Signal „Output 1“ (EIN), wenn alle Eingangssignale dem Vergleichswert entsprechen.

Das Signal „Output 1“ wird deaktiviert (AUS), sobald die Eingangssignale nicht mehr dem Vergleichswert entsprechen.

Es können 1 bis 8 Eingänge für die Eingangssignale konfiguriert werden.

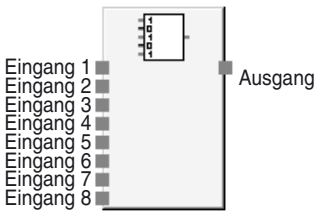
Parametereinstellungen

Einstellung	Einstellbereich	Standardeinstellung
Vergleichswert	00000000 bis 11111111 (Bit 0 bis Bit 7)	00000001

Optionale Eingangseinstellungen

Die Anzahl der Eingänge kann auf der Registerkarte „In/Out Setting“ des Eigenschaftendialogfelds der Logikfunktion auf einen Wert zwischen 1 und 8 eingestellt werden.

Einstellung	Einstellbereich	Standardeinstellung
Number of Inputs	1 bis 8	1



Funktionsblock „Komparator“ mit der maximal möglichen Zahl von Eingängen

Wahrheitstabelle

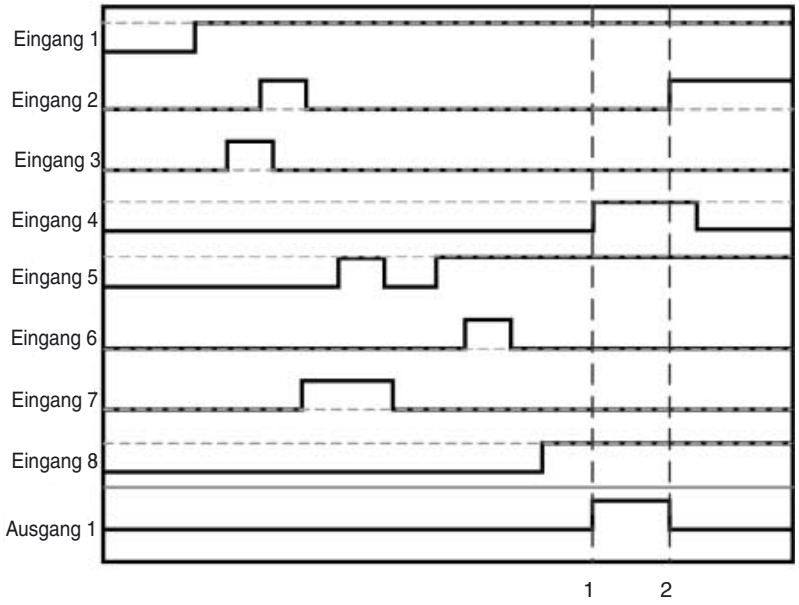
■ **Wahrheitstabelle für Komparatorprüfung (CV = Vergleichswert):**

Eingang 1	Eingang 2	Eingang 3	Eingang 4	Eingang 5	Eingang 6	Eingang 7	Eingang 8	Ausgang 1
≠ CV für Bit 0	×	×	×	×	×	×	×	0
×	≠ CV für Bit 1	×	×	×	×	×	×	0
×	×	≠ CV für Bit 2	×	×	×	×	×	0
×	×	×	≠ CV für Bit 3	×	×	×	×	0
×	×	×	×	≠ CV für Bit 4	×	×	×	0
×	×	×	×	×	≠ CV für Bit 5	×	×	0
×	×	×	×	×	×	≠ CV für Bit 6	×	0
×	×	×	×	×	×	×	≠ CV für Bit 7	0
= CV für Bit 0	= CV für Bit 1	= CV für Bit 2	= CV für Bit 3	= CV für Bit 4	= CV für Bit 5	= CV für Bit 6	= CV für Bit 7	1

0: AUS, 1: EIN, ?: wahlweise EIN oder AUS

Hinweis „= CV für Bit n“ bedeutet, dass das Bit dem Vergleichswert entspricht.
„≠ CV für Bit n“ bedeutet, dass das Bit nicht dem Vergleichswert entspricht.
„×“ bedeutet, dass der Status nicht anwendbar ist (kann übereinstimmen oder auch nicht).

Zeitablaufdiagramm



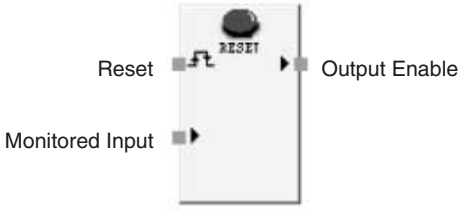
Die gestrichelten waagrechten Linien im obigen Diagramm repräsentieren den Vergleichswert für die einzelnen Eingänge.

1. Ausgang 1 wird aktiviert (EIN), wenn alle Eingangssignale dem Vergleichswert entsprechen.
2. Ausgang 1 wird deaktiviert (AUS), sobald eines der Eingangssignale nicht mehr dem Vergleichswert entspricht.

6-5 Befehlsreferenz: Funktionsblöcke

6-5-1 Funktionsblock: Rücksetzung

Diagramm



Standardbelegung (Ein- und Ausgänge)

Allgemeine Beschreibung

Der Ausgang „Output Enable“ wird auf EIN gesetzt, sobald das Rücksetzsignal am Eingang „Reset“ ordnungsgemäß gegeben wird, während die Eingangsbedingungen für den Funktionsblock aktiviert (auf EIN gesetzt) sind.

Dieser Funktionsblock kann genutzt werden, um ein automatisches Zurücksetzen der Maschine – beispielsweise beim Einschalten der Versorgungsspannung des Sicherheitsnetzwerk-Controllers NE1A, bei einem Wechsel des Betriebsmodus von „IDLE“ nach „RUN“ oder einer Signalisierung durch ein Sicherheitseingangsgerät – zu verhindern.

Bedingungen für die Aktivierung des Ausgangs „Output Enable“

- Der Eingang „Monitored Input“ sowie sämtliche verwendeten optionalen Eingänge müssen auf EIN gesetzt sein.
- Das Signal am Eingang „Restart“ muss ordnungsgemäß gegeben werden.

Bedingungen für die Aktivierung des Ausgangs „Static Release“

Der Eingang „Monitored Input“ sowie sämtliche verwendeten optionalen Eingänge müssen auf EIN gesetzt sein.

Bedingungen für die Aktivierung des Ausgangs „Reset Required Indication“

Wenn die folgenden Bedingungen erfüllt sind, liegt am Ausgang „Reset Required Indication“ ein 1-Hz-Impulssignal an.

- Der Eingang „Monitored Input“ sowie sämtliche verwendeten optionalen Eingänge müssen auf EIN gesetzt sein.
- Der Ausgang „Output Enable“ muss auf AUS gesetzt sein.

Wenn das Reset-Signal als „Low-High-Low“ konfiguriert wird, wird „Reset Required Indication“ aktiviert (EIN), sobald die nächste Bedingung erfüllt ist.

- Das Reset-Signal wird aktiviert (EIN).

Parametereinstellungen

Das Reset-Signal kann bei einem Sicherheitsnetzwerk-Controller NE1A ab Geräteversion 1.0 konfiguriert werden.

Einstellung	Einstellbereich	Standardeinstellung
Rücksetzsignal	• Low-High-Low • Ansteigende Flanke	Low-High-Low

Number of Inputs (Einstellung)

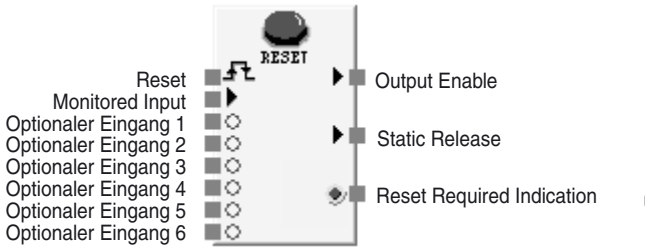
Die Anzahl der Eingänge kann auf der Registerkarte „In/Out Setting“ des Eigenschaftendialogfelds der Logikfunktion auf einen Wert zwischen 1 und 8 eingestellt werden.

Einstellung	Einstellbereich	Standardeinstellung
Number of Inputs	2 bis 8	2

Optionale Ausgangseinstellungen

Die nachstehend gezeigten Ausgänge können im Programm verwendet werden. Um einen dieser Ausgänge zu aktivieren, muss das Kontrollkästchen auf der Registerkarte „Out Point“ des Eigenschaftendialogfelds des Funktionsblocks aktiviert werden.

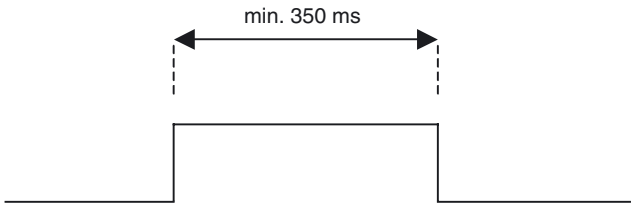
- Static Release
- Reset Required Indication



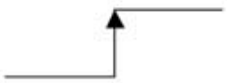
Funktionsblock „Reset“ mit der maximal möglichen Zahl von Eingängen und Ausgängen

Rücksetzsignal

Das Rücksetzsignal muss den folgenden Bedingungen genügen:

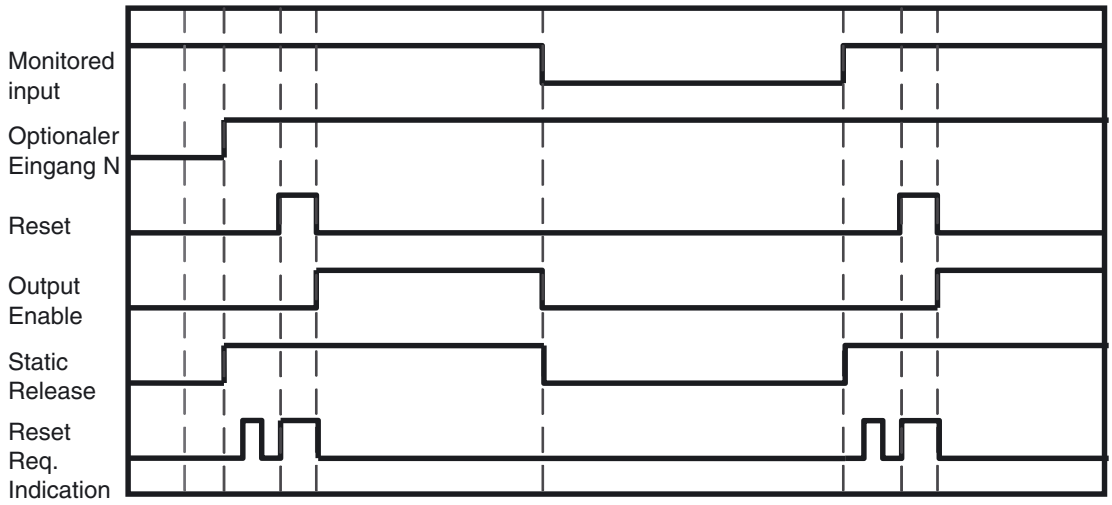


Bei Sicherheitsnetzwerk-Controllern NE1A ab Geräteversion 1.0 kann die steigende Flanke (Low-to-High) ausgewählt werden. Zur Aktivierung dieses Signals setzen Sie auf der Registerkarte „Parameter“ im Dialogfeld „Funktionsblockeigenschaften“ den Eintrag *Reset Signal* auf *Rising Edge*.

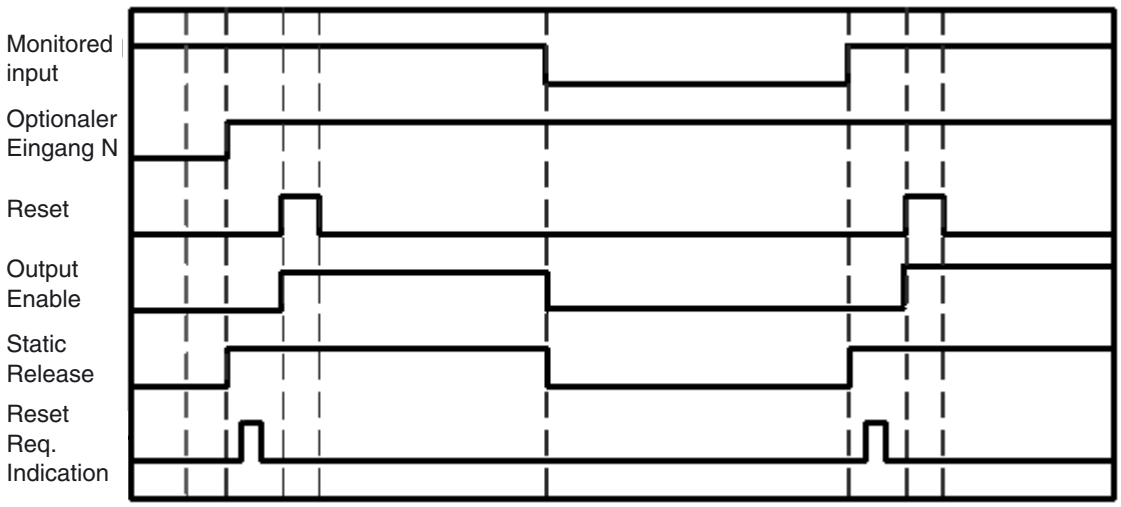


Zeitablaufdiagramm

Reset-Signal auf Low-High-Low konfiguriert:

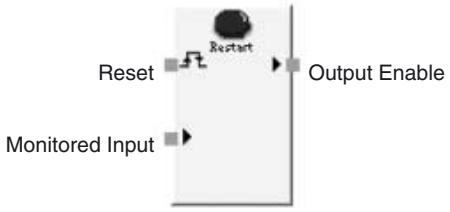


Reset Signal auf „Rising Edge“ (steigende Flanke) konfiguriert:



6-5-2 Funktionsblock: Restart

Diagramm



Standardbelegung (Ein- und Ausgänge)

Allgemeine Beschreibung

Der Ausgang „Output Enable“ wird auf EIN gesetzt, sobald das Neustartsignal am Eingang „Restart“ ordnungsgemäß gegeben wird, während die Eingangsbedingungen für den Funktionsblock aktiviert (auf EIN gesetzt) sind.

Dieser Funktionsblock kann genutzt werden, um einen automatischen Neustart der Maschine – beispielsweise beim Einschalten der Versorgungsspannung des Sicherheitsnetzwerk-Controllers NE1A, bei einem Wechsel des Betriebsmodus von „IDLE“ nach „RUN“ oder einer Signalisierung durch ein Sicherheitseingangsgerät – zu verhindern.

Vom Verhalten her sind die Funktionsblöcke „Reset“ und „Restart“ äquivalent.

Bedingungen für die Aktivierung des Ausgangs „Output Enable“

- Der Eingang „Monitored Input“ sowie sämtliche verwendeten optionalen Eingänge müssen auf EIN gesetzt sein.
- Das Signal am Eingang „Restart“ muss ordnungsgemäß gegeben werden.

Bedingungen für die Aktivierung des Ausgangs „Static Release“

Der Eingang „Monitored Input“ sowie sämtliche verwendeten optionalen Eingänge müssen auf EIN gesetzt sein.

Bedingungen für die Aktivierung des Ausgangs „Restart Required Indication“

Wenn die folgenden Bedingungen erfüllt sind, liegt am Ausgang „Restart Required Indication“ ein 1-Hz-Impulssignal an.

- Der Eingang „Monitored Input“ sowie sämtliche verwendeten optionalen Eingänge müssen auf EIN gesetzt sein.
- Der Ausgang „Output Enable“ muss auf AUS gesetzt sein.

Wenn das Reset-Signal als „Low-High-Low“ konfiguriert wird, wird „Reset Required Indication“ aktiviert (EIN), sobald die nächste Bedingung erfüllt ist.

- Der Eingang „Restart“ ist auf EIN gesetzt.

Parametereinstellungen

Das Reset-Signal kann bei einem Sicherheitsnetzwerk-Controller NE1A ab Geräteversion 1.0 konfiguriert werden.

Einstellung	Einstellbereich	Standardeinstellung
Rücksetzsignal	• Low-High-Low • Ansteigende Flanke	Low-High-Low

Number of Inputs (Einstellung)

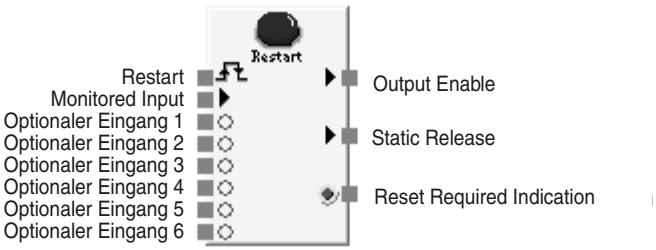
Die Anzahl der Eingänge kann auf der Registerkarte „In/Out Setting“ des Eigenschaftendialogfelds der Logikfunktion auf einen Wert zwischen 1 und 8 eingestellt werden.

Einstellung	Einstellbereich	Standardeinstellung
Number of Inputs	2 bis 8	2

Optionale Ausgangseinstellungen

Die nachstehend gezeigten Ausgänge können im Programm verwendet werden. Um einen dieser Ausgänge zu aktivieren, muss das Kontrollkästchen auf der Registerkarte „Out Point“ des Eigenschaftendialogfelds des Funktionsblocks aktiviert werden.

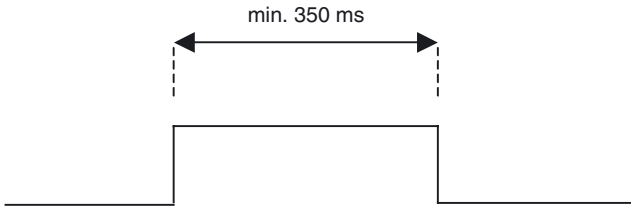
- Static Release
- Restart Required Indication



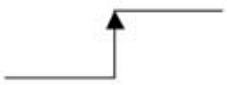
Funktionsblock „Restart“ mit der maximal möglichen Zahl von Eingängen und Ausgängen

Neustartsignal

Das Neustartsignal muss den folgenden Bedingungen genügen:

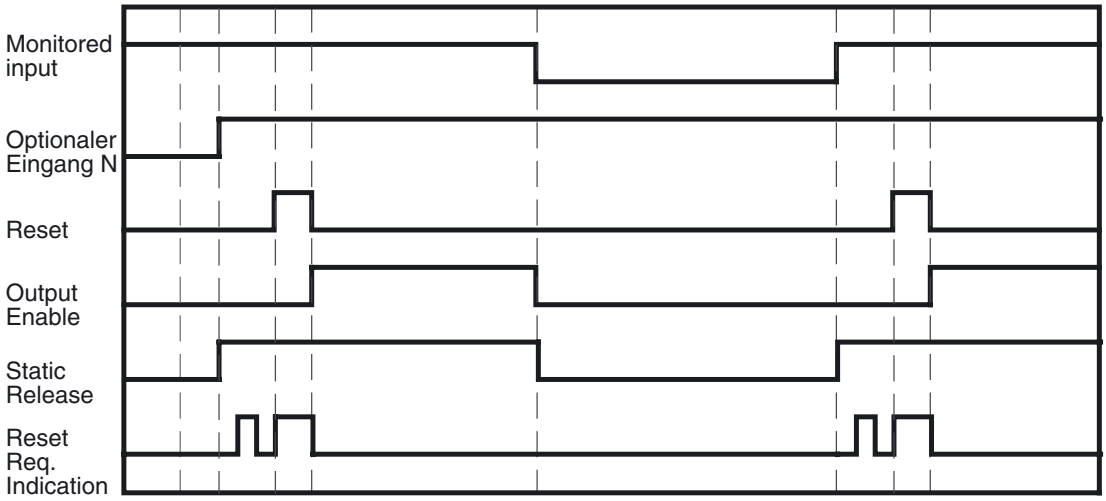


Bei Sicherheitsnetzwerk-Controllern NE1A ab Geräteversion 1.0 kann die steigende Flanke (Low-to-High) ausgewählt werden. Zur Aktivierung dieses Signals setzen Sie auf der Registerkarte „Parameter“ im Dialogfeld „Funktionsblockeigenschaften“ den Eintrag *Reset Signal* auf *Rising Edge*.

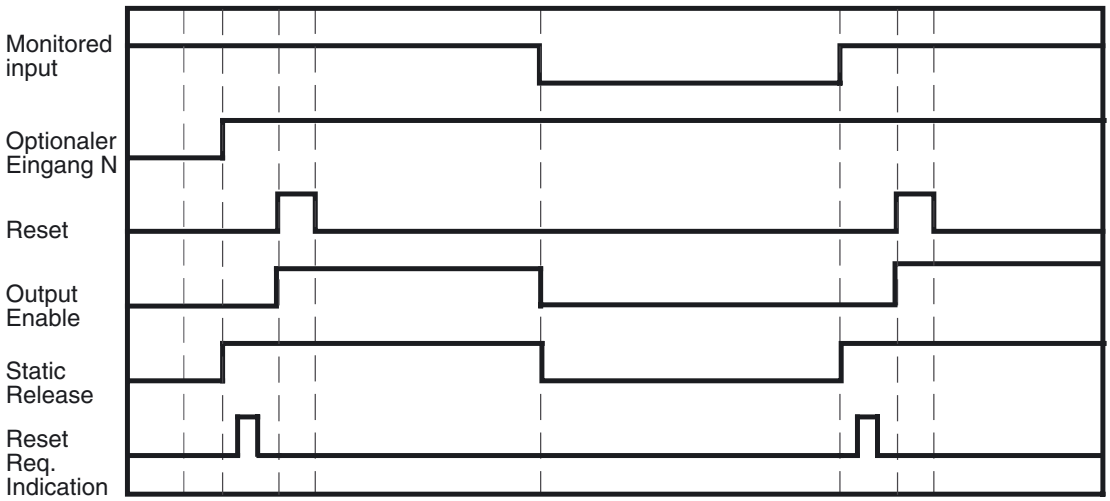


Zeitablaufdiagramm

Reset-Signal auf Low-High-Low konfiguriert:

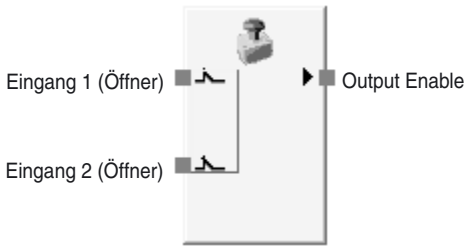


Reset Signal auf „Rising Edge“ (steigende Flanke) konfiguriert:



6-5-3 Funktionsblock: NOT-AUS-Taster-Überwachung

Diagramm



Standardbelegung (Ein- und Ausgänge)

Allgemeine Beschreibung

Der Funktionsblock für die NOT-AUS-Taster-Überwachung ermöglicht die Überwachung eines NOT-AUS-Tasters.

Der Ausgang „Output Enable“ wird auf EIN gesetzt, wenn aufgrund der Eingangssignale des überwachten NOT-AUS-Tasters feststeht, dass dieser nicht betätigt ist. Der Ausgang „Output Enable“ wird auf AUS gesetzt, wenn aufgrund der Eingangssignale des überwachten NOT-AUS-Tasters feststeht, dass dieser betätigt ist oder wenn innerhalb des Funktionsblocks ein Fehler festgestellt wird.

WICHTIG NOT-AUS-Anwendungen benötigen eine manuelle Rücksetzfunktion. Bei Verwendung des Funktionsblocks für die NOT-AUS-Taster-Überwachung muss auch die Logikfunktion „Reset“ verwendet werden.
Programmierbeispiele finden Sie unter *A-1-1 NOT-AUS-Anwendung: Zweikanal-Modus mit manueller Rücksetzung*.

Parametereinstellungen

Einstellung	Einstellbereich	Standardeinstellung
Input Type	Single Channel Dual Channel Equivalent Dual Channel Complementary	Dual Channel Equivalent
Discrepancy Time	0 bis 30 s (in 10-ms-Schritten) Bei der Einstellung 0 erfolgt keine Überprüfung der Diskrepanzzeit.	30 ms

Die Diskrepanzzeit muss größer sein als die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A.

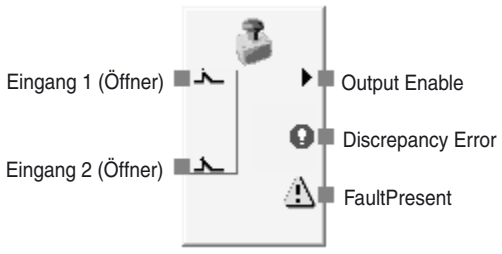
Optionaler Ausgang

Bei der Programmierung kann auch der folgende Fehlerausgang genutzt werden. Damit dieser optionale Ausgang im Logik-Editor angezeigt wird, muss das Kontrollkästchen auf der Registerkarte „Out Point“ des Eigenschaftendialogfelds des Funktionsblocks aktiviert werden.

- Discrepancy Error

Einstellung „Use Fault Present“

Bei der Programmierung kann auch der Ausgang „Fault Present“ genutzt werden. Damit dieser optionale Ausgang im Logik-Editor angezeigt wird, muss das Kontrollkästchen „Fault Present“ auf der Registerkarte „Out Point“ des Eigenschaftendialogfelds des Funktionsblocks aktiviert werden.



Funktionsblock für die NOT-AUS-Taster-Überwachung mit maximaler Eingangs- und Ausgangszahl

Wahrheitstabellen

Einstellung: Single Channel

Eingang 1 (Öffner)	Output Enable
0	0
1	1

0: AUS, 1: EIN

Einstellung: Dual Channel Equivalent

Eingang 1 (Öffner)	Eingang 2 (Öffner)	Output Enable
0	0	0
0	1	0
1	0	0
1	1	1

0: AUS, 1: EIN

Einstellung: Dual Channel Complementary

Eingang 1 (Öffner)	Eingang 2 (Schließer)	Output Enable
0	0	0
0	1	0
1	0	1
1	1	0

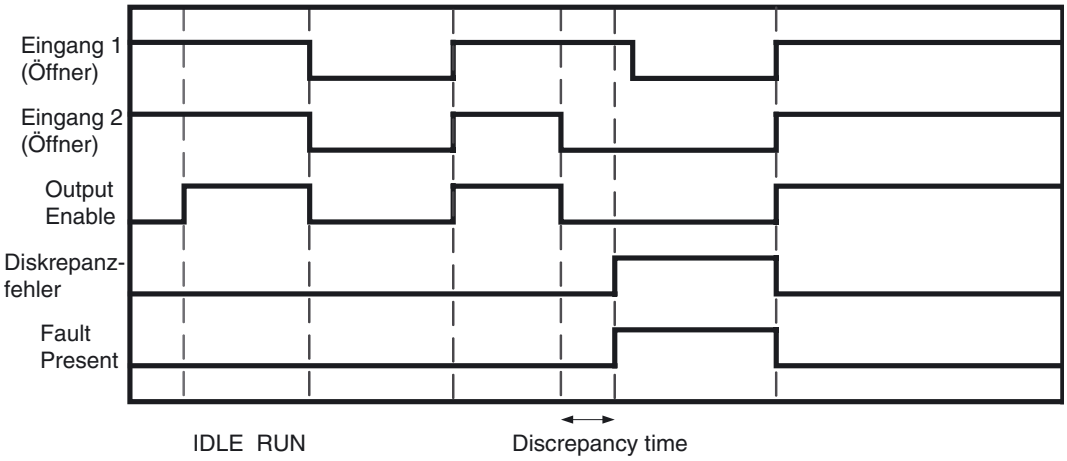
0: AUS, 1: EIN

Fehlerbehandlung und Zurücksetzen des Fehlerzustands

Fehler zustands	Verhalten bei Fehlererkennung			Zurücksetzen des Fehler-zustand
	Output Enable	Fault Present	Fehlerausgang	
Diskrepanz-fehler	AUS (Sicher-heitszu-stand)	EIN	Ausgang „Discrepancy Error“: EIN	Beheben Sie die Ursache des Fehlers, und gehen Sie dann wie folgt vor: 1. Setzen Sie die Eingänge auf AUS und dann wieder auf EIN, oder 2. ändern Sie den Betriebs-modus des Sicherheitsnetz-werk-Controllers NE1A nach IDLE und dann wieder nach RUN.

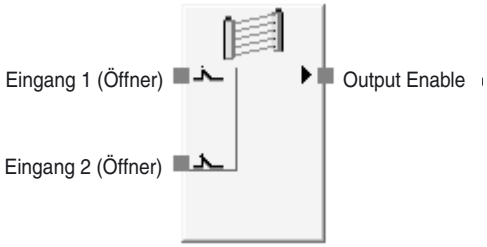
Zeitablaufdiagramm

Einstellung: Dual Channel Equivalent



6-5-4 Funktionsblock: Lichtgitter-Überwachung

Diagramm



Standardbelegung (Ein- und Ausgänge)

Allgemeine Beschreibung

Der Funktionsblock für die Lichtgitter-Überwachung ermöglicht die Überwachung eines Sicherheitslichtgitters der Kategorie 4.

Der Ausgang „Output Enable“ wird auf EIN gesetzt, wenn aufgrund der Eingangssignale des überwachten Sicherheitslichtgitters feststeht, dass der Strahlengang nicht unterbrochen ist. Der Ausgang „Output Enable“ wird auf AUS gesetzt, wenn aufgrund der Eingangssignale des überwachten Sicherheitslichtgitters feststeht, dass der Strahlengang unterbrochen ist oder wenn innerhalb des Funktionsblocks ein Fehler festgestellt wird.

Parametereinstellungen

Einstellung	Einstellbereich	Standardeinstellung
Input type	Dual Channel Equivalent Dual Channel Complementary	Dual Channel Equivalent
Discrepancy time	0 bis 30 s (in 10-ms-Schritten) Bei der Einstellung 0 erfolgt keine Überprüfung der Diskrepanzzeit.	30 ms

Die Diskrepanzzeit muss größer sein als die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A.

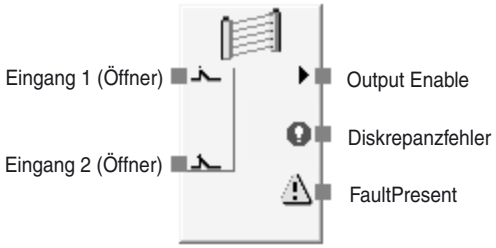
Optionaler Ausgang

Bei der Programmierung kann auch der folgende Fehlerausgang genutzt werden. Damit dieser optionale Ausgang im Logik-Editor angezeigt wird, muss das Kontrollkästchen auf der Registerkarte „Out Point“ des Eigenschaftendialogfelds des Funktionsblocks aktiviert werden.

- Discrepancy Error

Einstellung „Use Fault Present“

Bei der Programmierung kann auch der Ausgang „Fault Present“ genutzt werden. Damit dieser optionale Ausgang im Logik-Editor angezeigt wird, muss das Kontrollkästchen „Fault Present“ auf der Registerkarte „Out Point“ des Eigenschaftendialogfelds des Funktionsblocks aktiviert werden.



Funktionsblock für die Lichtgitter-Überwachung mit maximaler Eingangs- und Ausgangszahl

Wahrheitstabellen

Einstellung: Dual Channel Equivalent

Eingang 1 (Öffner)	Eingang 2 (Öffner)	Output Enable
0	0	0
0	1	0
1	0	0
1	1	1

0: AUS, 1: EIN

Einstellung: Dual Channel Complementary

Eingang 1 (Öffner)	Eingang 2 (Schließer)	Output Enable
0	0	0
0	1	0
1	0	1
1	1	0

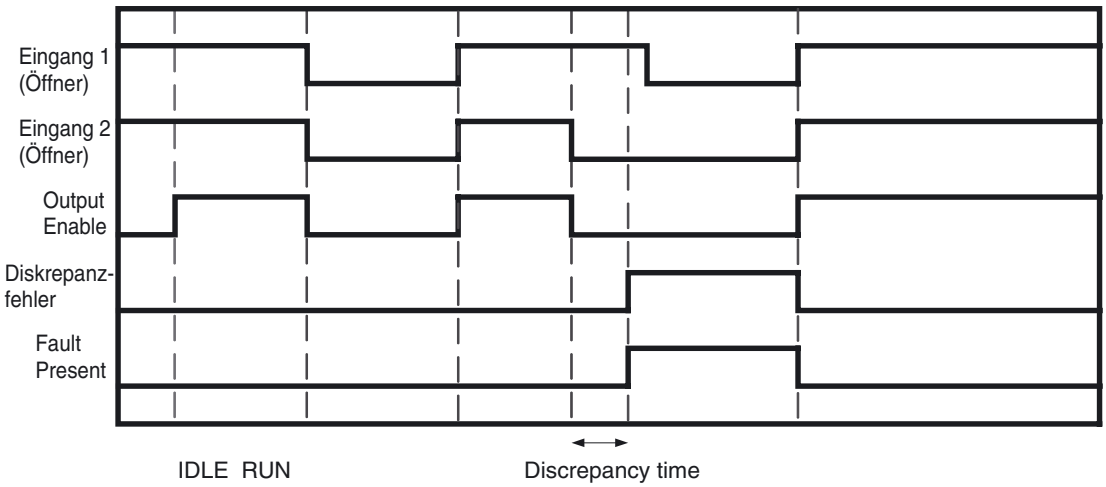
0: AUS, 1: EIN

Fehlerbehandlung und Zurücksetzen des Fehlerzustands

Fehler zustands	Verhalten bei Fehlererkennung			Zurücksetzen des Fehlerzustand
	Output Enable	Fault Present	Fehler-ausgang	
Diskrepanz-fehler	AUS (Sicher-heitszu-stand)	EIN	Ausgang „Dis-crepancy Error“: EIN	Beheben Sie die Ursache des Fehlers, und gehen Sie dann wie folgt vor: 1. Setzen Sie die Eingänge auf AUS und dann wieder auf EIN, oder 2. ändern Sie den Betriebsmo-dus des Sicherheitsnetzwerk-Controllers NE1A nach IDLE und dann wieder nach RUN.

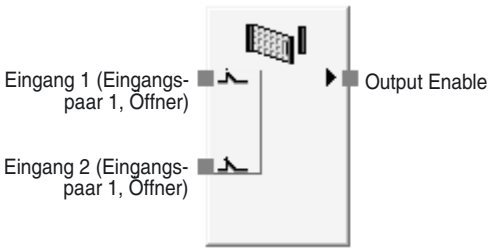
Zeitablaufdiagramm

Einstellung: Dual Channel Equivalent



6-5-5 Funktionsblock: Sicherheitstür-Überwachung

Diagramm



Standardbelegung (Ein- und Ausgänge)

Allgemeine Beschreibung

Der Funktionsblock für die Sicherheitstür-Überwachung ermöglicht die Überwachung einer Sicherheitstür anhand des Eingangssignals eines Sicherheitstürschalters oder eines an der Tür montierten Sicherheitspositionsschalters.

Der Ausgang „Output Enable“ wird auf EIN gesetzt, wenn aufgrund der Eingangssignale des Schalters feststeht, dass die Tür geschlossen ist. Der Ausgang „Output Enable“ wird auf AUS gesetzt, wenn aufgrund der Eingangssignale des überwachten NOT-AUS-Tasters feststeht, dass dieser betätigt ist oder wenn innerhalb des Funktionsblocks ein Fehler festgestellt wird.

Funktionstests

Bestimmte Sicherheitstüranwendungen (z. B. Sicherheitstüranwendungen der Kategorie 2) erfordern eine physikalische Überprüfung der dauerhaft einwandfreien Funktion des Sicherheitsgeräts.

Ist die Funktionstest-Option für den Funktionsblock für die Sicherheitstür-Überwachung aktiviert, kann ein Sicherheitstürtest als zusätzliche Bedingung für die Aktivierung des Ausgangssignals „Output Enable“ eingesetzt werden. Bei der Durchführung des Sicherheitstürtests muss die Tür geöffnet und wieder geschlossen werden

Ist die Funktionstest-Option für den Funktionsblock für die Sicherheitstür-Überwachung aktiviert, muss in folgenden Fällen ein Sicherheitstürtest durchgeführt werden:

1. Beim Systemstart
   Beim Start des Sicherheitsnetzwerk-Controllers NE1A (d. h. beim Übergang vom Betriebsmodus IDLE in den Betriebsmodus RUN) muss ein Sicherheitstürtest durchgeführt werden. Nach erfolgreicher Durchführung des Tests wird das das Ausgangssignal „Output Enable“ auf EIN gesetzt.
2. Bei einer Funktionstestanforderung durch die Maschine
   Ein Sicherheitstürtest muss durchgeführt werden, nachdem das Eingangssignal „Function Test“ des Sicherheitsnetzwerk-Controllers NE1A durch die Maschine auf EIN gesetzt wurde. Die Durchführung des Tests muss abgeschlossen sein, bevor dieses Eingangssignal ein weiteres Mal auf EIN gesetzt wurde. Wird das Eingangsignal „Function Test“ ein weiteres Mal auf EIN gesetzt, bevor der Sicherheitstürtest erfolgreich abgeschlossen wurde, tritt ein Fehler auf und der Ausgang „Output Enable“ des Funktionsblocks wird nicht auf EIN gesetzt. Zudem wird das Ausgangssignal „Function Test Error“ auf EIN gesetzt.
3. Bei Erkennung eines Fehlers im Funktionsblock für die Sicherheitstür-Überwachung
   Nach dem Auftreten eines Funktionstestfehlers, eines Diskrepanzfehlers oder eines anderen Fehlers im Funktionsblock muss – nach Behebung der Fehlerursache – ein Sicherheitstürtest durchgeführt werden.

Ist die Durchführung eines Sicherheitstürtests erforderlich, wird der Ausgang „Function Test Required“ des Funktionsblocks für die Sicherheitstür-Überwachung so lange auf EIN gesetzt, bis der Sicherheitstürtest erfolgreich durchgeführt wurde.

Parametereinstellungen

Einstellung	Einstellbereich	Standard-einstellung
Input Type	Single Channel Dual Channel Equivalent (1 Pair) Dual Channel Complementary (1 Pair) Two Dual Channel Equivalent (2 Pairs) Two Dual Channel Complementary (2 Pairs)	Dual Channel Equivalent (1 Pair)
Function Test	No Function Test/Function Test Required	No Function Test
Discrepancy Time Pair 1	0 bis 30 s (in 10-ms-Schritten) Bei der Einstellung 0 erfolgt keine Überprüfung der Diskrepanzzeit.	30 ms
Discrepancy Time Pair 2		
Synchronization Time	0 bis 30 s (in 10-ms-Schritten) Bei der Einstellung 0 erfolgt keine Überprüfung der Synchronisationszeit.	300 ms

Diskrepanzzeit und Synchronisationszeit müssen größer sein als die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A.

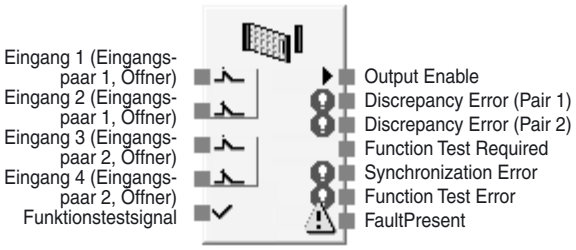
Optionale Ausgangseinstellungen

Bei der Programmierung können auch die folgenden Ausgänge genutzt werden. Um einen dieser optionalen Ausgänge zu aktivieren, muss das Kontrollkästchen auf der Registerkarte „Out Point“ des Eigenschaftendialogfelds des Funktionsblocks aktiviert werden.

Discrepancy Error (Pair 1)
Discrepancy Error (Pair 2)
Function Test Required
Synchronization Error
Function Test Error

Einstellung „Use Fault Present“

Bei der Programmierung kann auch der Ausgang „Fault Present“ genutzt werden. Damit dieser optionale Ausgang im Logik-Editor angezeigt wird, muss das Kontrollkästchen „Fault Present“ auf der Registerkarte „Out Point“ des Eigenschaftendialogfelds des Funktionsblocks aktiviert werden.



Funktionsblock für die Lichtgitter-Überwachung mit maximaler Eingangs- und Ausgangszahl

Wahrheitstabellen

Einstellung: Single Channel

Eingang 1 (Eingangspaar 1, Öffner)	Output Enable
0	0
1	1

0: AUS, 1: EIN

Einstellung: Dual Channel Equivalent (1 Pair)

Eingang 1 (Eingangspaar 1, Öffner)	Eingang 2 (Eingangspaar 1, Öffner)	Output Enable
0	0	0
0	1	0
1	0	0
1	1	1

0: AUS, 1: EIN

Einstellung: Dual Channel Complementary (1 Pair)

Eingang 1 (Eingangspaar 1, Öffner)	Eingang 2 (Eingangspaar 1, Schließer)	Output Enable
0	0	0
0	1	0
1	0	1
1	1	0

0: AUS, 1: EIN

Einstellung: Two Dual Channel Equivalent (2 Pairs)

Eingang 1 (Eingangspaar 1, Öffner)	Eingang 2 (Eingangspaar 1, Öffner)	Eingang 3 (Eingangspaar 2, Öffner)	Eingang 4 (Eingangspaar 2, Öffner)	Output Enable
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	0
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	1

0: AUS, 1: EIN

Einstellung: Two Dual Channel Complementary (2 Pairs)

Eingang 1 (Eingangspaar 1, Öffner)	Eingang 2 (Eingangspaar 1, Schließer)	Eingang 3 (Eingangspaar 2, Öffner)	Eingang 4 (Eingangspaar 2, Schließer)	Output Enable
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	1
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

0: AUS, 1: EIN

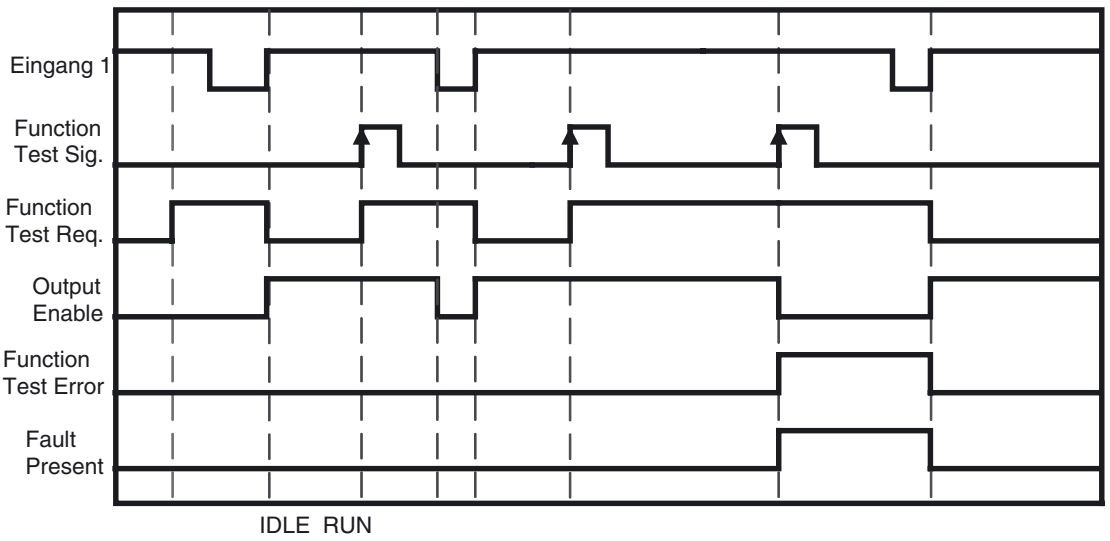
Fehlerbehandlung und Zurücksetzen des Fehlerzustands

Fehler zustand	Verhalten bei Fehlererkennung			Zurücksetzen des Fehlerzustands
	Output Enable	Fault Present	Fehlerausgang	
Diskrepanzfehler Eingangspaar 1	AUS (Sicherheitszustand)	EIN	Discrepancy Error (Pair 1): EIN	1. Funktionstest deaktiviert Beheben Sie die Ursache des Fehlers, und setzen Sie die Eingänge auf AUS und dann wieder auf EIN (siehe Hinweis), oder ändern Sie den Betriebsmodus des Sicherheitsnetzwerk-Controllers NE1A nach IDLE und dann wieder nach RUN. 2. Function Test Required Falls „Function Test Required“ aktiv ist: Beheben Sie die Ursache des Fehlers, und setzen Sie die Eingänge auf EIN, dann auf AUS und dann wieder auf EIN (entspricht der Durchführung des Sicherheitstürtests). Falls „Function Test Required“ nicht aktiv ist: Beheben Sie die Ursache des Fehlers, und setzen Sie die Eingänge auf AUS und dann wieder auf EIN.
Diskrepanzfehler Eingangspaar 2			Discrepancy Error (Pair 2): EIN	
Funktionstestfehler Zwischen zwei aufeinander folgenden Signalen am Eingang „Function Test“ erfolgte keine erfolgreiche Durchführung des Sicherheitstürtests.			Function Test Error: EIN	
Synchronisationsfehler			Synchronization Error: EIN	

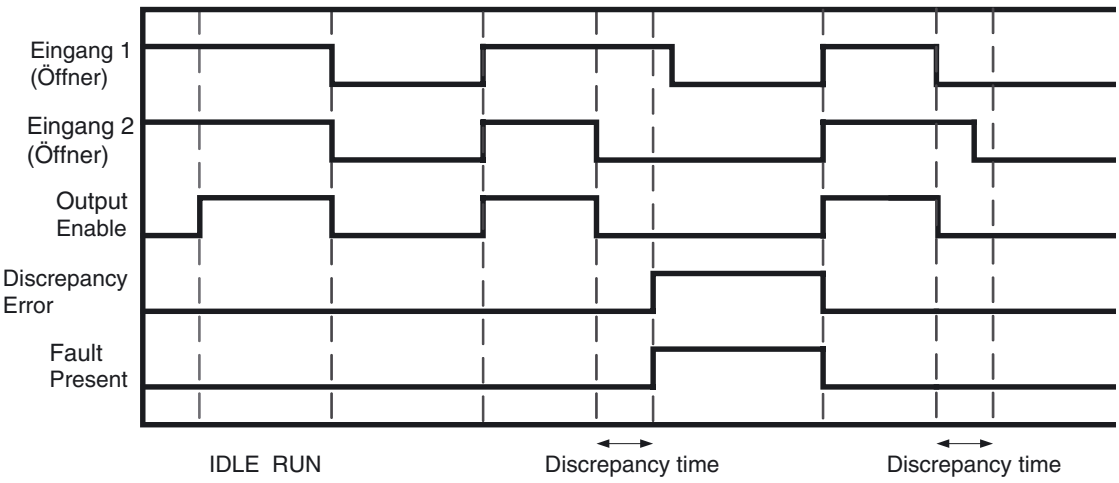
Hinweis Tritt bei Verwendung einer der Eingangsarten „Dual Channel Equivalent (2 Pairs)“ oder „Dual Channel Complementary (2 Pairs)“ ein Diskrepanzfehler auf, müssen zum Zurücksetzen des Fehlers beide Eingangspaare auf AUS und dann wieder auf EIN gesetzt werden.

Signalverhalten

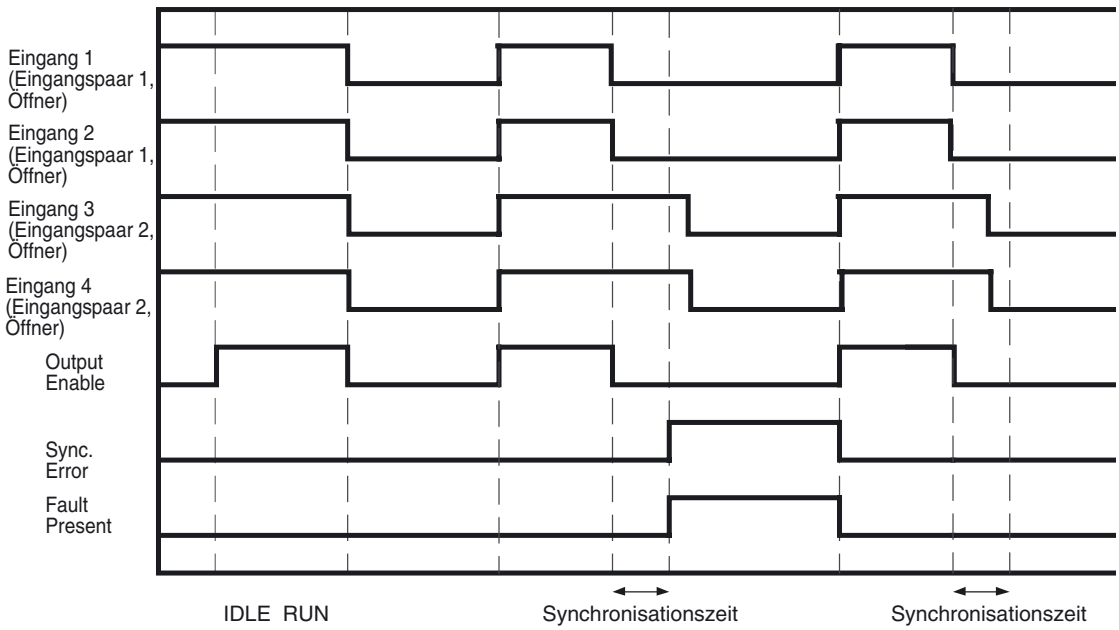
Single Channel, Funktionstest aktiviert



Dual Channel Equivalent, Funktionstest deaktiviert

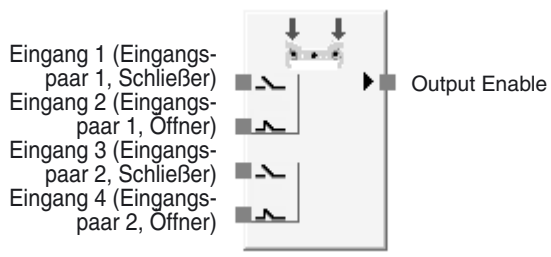


Dual Channel Equivalent (2 Pairs), Funktionstest deaktiviert



6-5-6 Funktionsblock: Zweihandsteuerung

Diagramm


Eingang 1 (Eingangs-paar 1, Schließer)
Eingang 2 (Eingangs-paar 1, Öffner)
Eingang 3 (Eingangs-paar 2, Schließer)
Eingang 4 (Eingangs-paar 2, Öffner)
Output Enable

Standardbelegung (Ein- und Ausgänge)

Allgemeine Beschreibung

Der Funktionsblock für die Zweihandsteuerung ermöglicht die Überwachung einer Zweihandsteuerung.

Dieser Funktionsblock eignet sich für die Verwendung mit einem geeigneten Typ-IIIC-Zweihandschalter (EN 574: *Zweihandschaltungen, funktionelle Aspekte – Gestaltungsleitsätze).*

Der Ausgang „Output Enable" wird nur dann auf EIN gesetzt, wenn beide Eingangssignale vom Zweihandschalter auf EIN gesetzt und die Bedingungen der EN 574 erfüllen. Der Ausgang „Output Enable" wird auf AUS gesetzt, wenn die Eingangssignale vom Zweihandschalter die Bedingungen der EN 574 nicht erfüllen, mindestens eines der beiden Eingangssignale auf AUS gesetzt ist oder innerhalb des Funktionsblocks ein Fehler festgestellt wird.

Parametereinstellungen

Einstellung	Einstellbereich	Standardeinstellung
Diskrepanzzeit Paar 1	0 bis 500 ms (in 10-ms-Schritten)	30 ms
Diskrepanzzeit Paar 2		

Die Diskrepanzzeiten müssen größer sein als die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A

Optionale Ausgangseinstellungen

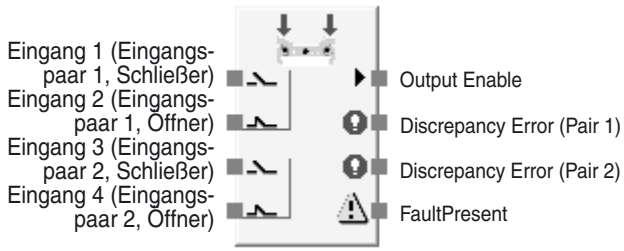
Bei der Programmierung können auch die folgenden Fehlerausgänge genutzt werden. Um einen dieser optionalen Ausgänge zu aktivieren, muss das Kontrollkästchen auf der Registerkarte „Out Point“ des Eigenschaftendialogfelds des Funktionsblocks aktiviert werden.

Discrepancy Error (Pair 1)

Discrepancy Error (Pair 2)

Einstellung „Use Fault Present“

Bei der Programmierung kann auch der Ausgang „Fault Present“ genutzt werden. Damit dieser optionale Ausgang im Logik-Editor angezeigt wird, muss das Kontrollkästchen „Use Fault Present“ auf der Registerkarte „Out Point“ des Eigenschaftendialogfelds des Funktionsblocks aktiviert werden.



Funktionsblock für die Zweihandsteuerung mit maximaler Eingangs- und Ausgangszahl

Wahrheitstabelle

Eingang 1 (Eingangspaar 1, Schließer)	Eingang 2 (Eingangspaar 1, Öffner)	Eingang 3 (Eingangspaar 2, Schließer)	Eingang 4 (Eingangspaar 2, Öffner)	Output Enable
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	1
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

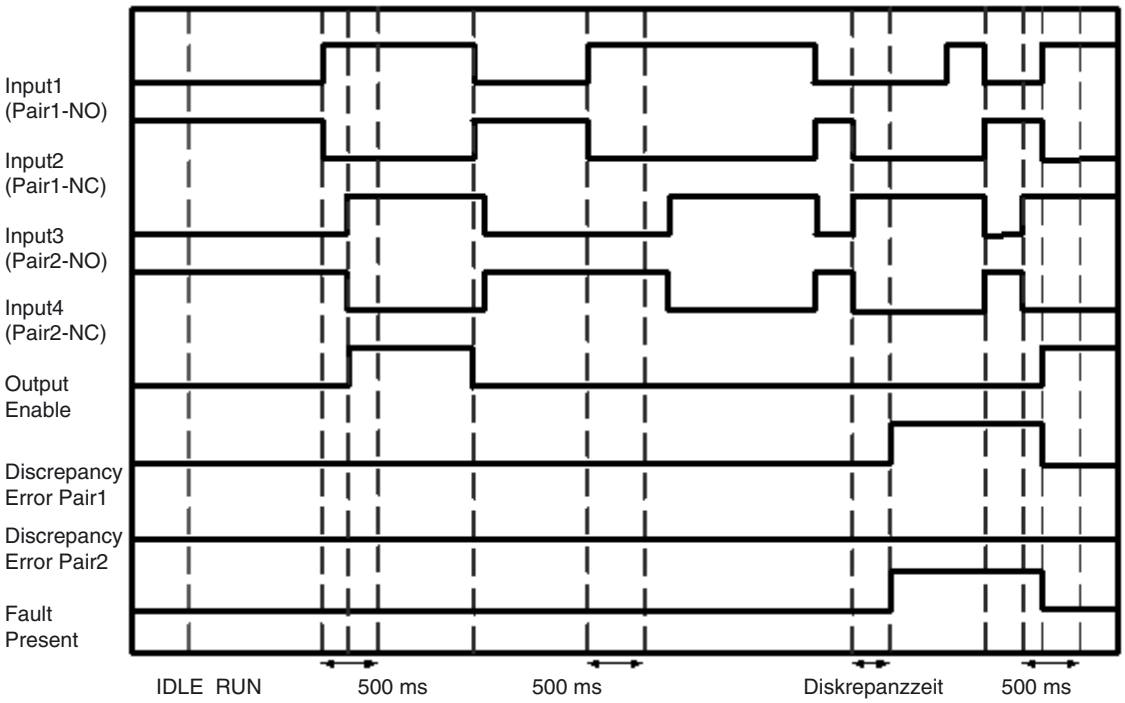
0: AUS, 1: EIN

Fehlerbehandlung und Zurücksetzen des Fehlerzustands

Fehler zustand	Verhalten bei Fehlererkennung			Zurücksetzen des Fehlerzustands
	Output Enable	Fault Present	Fehlerausgang	
Diskrepanzfehler Eingangspaar 1	AUS (Sicherheitszustand)	EIN	Discrepancy Error (Pair 1): EIN	Beheben Sie die Ursache des Fehlers, und gehen Sie dann wie folgt vor: 1. Setzen Sie die Eingänge beider Eingangspaare auf AUS und dann wieder auf EIN, oder 2. ändern Sie den Betriebsmodus des Sicherheitsnetzwerk-Controllers NE1A nach IDLE und dann wieder nach RUN.
Diskrepanzfehler Eingangspaar 2			Discrepancy Error (Pair 2): EIN	

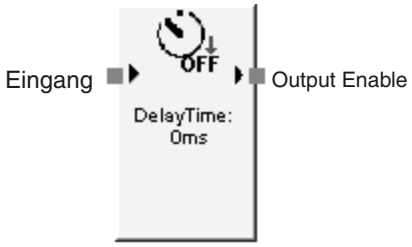
Hinweis Der Ausgang „Output Enable“ wird nicht auf EIN gesetzt, wenn die Anforderungen an die Synchronisationszeit nicht erfüllt sind, d. h. die Betätigung der beiden Schalter des Zweihandschalters mit einem zeitlichen Abstand von mehr als 500 ms erfolgt. Dies wird jedoch **nicht** als Fehler angesehen.

Zeitablaufdiagramm



6-5-7 Funktionsblock: Ausschaltverzögerung

Diagramm



Allgemeine Beschreibung

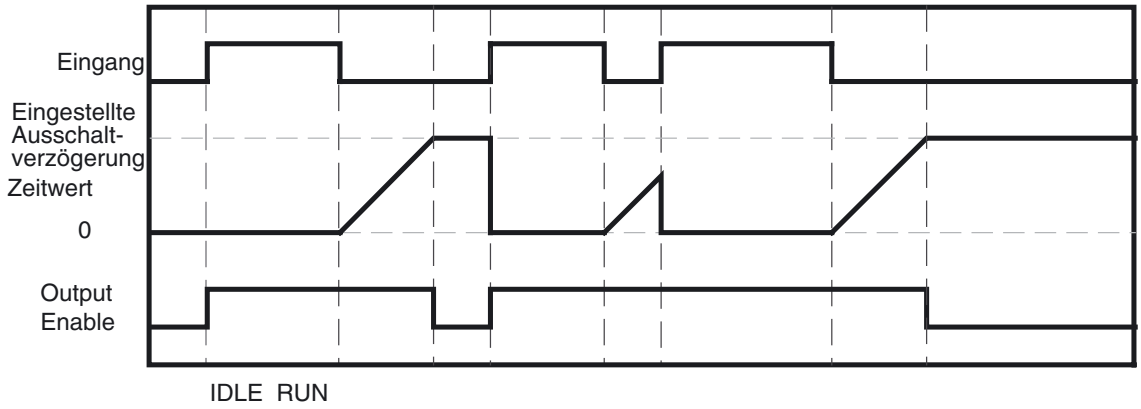
Der Ausschaltverzögerungs-Funktionsblock ermöglicht die Realisierung einer Ausschaltverzögerung von 0 bis 300 s (in 10-ms-Schritten einstellbar).

Parametereinstellungen

Einstellung	Einstellbereich	Standardeinstellung
OFF-delay Time	0 bis 300 s (in 10-ms-Schritten)	0 ms

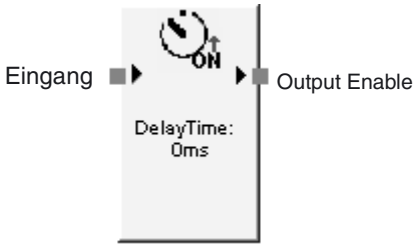
Die Ausschaltverzögerungszeit muss größer sein als die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A.

Zeitablaufdiagramm



6-5-8 Funktionsblock: Einschaltverzögerung

Diagramm



Allgemeine Beschreibung

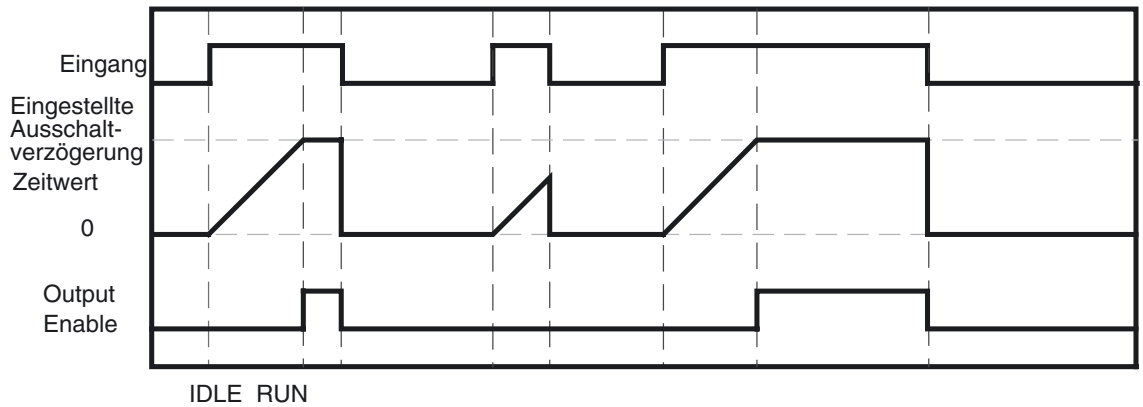
Der Einschaltverzögerungs-Funktionsblock ermöglicht die Realisierung einer Einschaltverzögerung von 0 bis 300 s (in 10-ms-Schritten einstellbar).

Parametereinstellungen

Einstellung	Einstellbereich	Standardeinstellung
ON-delay Time	0 bis 300 s (in 10-ms-Schritten)	0 ms

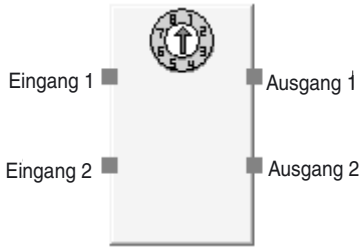
Die Einschaltverzögerungszeit muss größer sein als die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A.

Zeitablaufdiagramm



6-5-9 Funktionsblock: Betriebsartenwahlschalter

Diagramm



Standardbelegung (Ein- und Ausgänge)

Allgemeine Beschreibung

Der Betriebsartenwahlschalter-Funktionsblock ermöglicht die Überwachung eines Betriebsartenauswahlschalters.

Bei dem an diesen Funktionsblock angeschlossenen Betriebsartenwahlschalter muss es sich um einen 1:n-Schalter (immer nur einer von n Kontakten ist auf EIN gesetzt) handeln. Der Funktionsblock unterstützt bis zu acht Eingänge (samt den entsprechenden Ausgängen).

Der dem auf EIN gesetzten Eingang entsprechende Ausgang wird auf EIN gesetzt. Wird im Funktionsblock ein Fehler erkannt, werden alle Ausgänge auf AUS gesetzt.

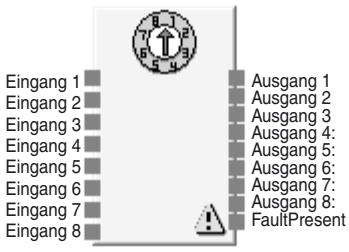
Optionale Ausgangseinstellungen

Die Anzahl der Eingänge kann auf der Registerkarte „In/Out Setting“ des Eigenschaftendialogfelds des Funktionsblocks auf einen Wert zwischen 2 und 8 eingestellt werden.

Einstellung	Einstellbereich	Standard-einstellung
Number of Inputs	2 bis 8	2
Number of Outputs	2 bis 8	2

Einstellung „Use Fault Present“

Bei der Programmierung kann auch der Ausgang „Fault Present“ genutzt werden. Damit dieser optionale Ausgang im Logik-Editor angezeigt wird, muss das Kontrollkästchen „Fault Present“ auf der Registerkarte „In/Out Setting“ des Eigenschaftendialogfelds des Funktionsblocks aktiviert werden.



Betriebsartenauswahlschalter-Funktionsblock mit der maximal möglichen Zahl von Eingängen

Wahrheitstabelle

Eingänge								Ausgänge							
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1

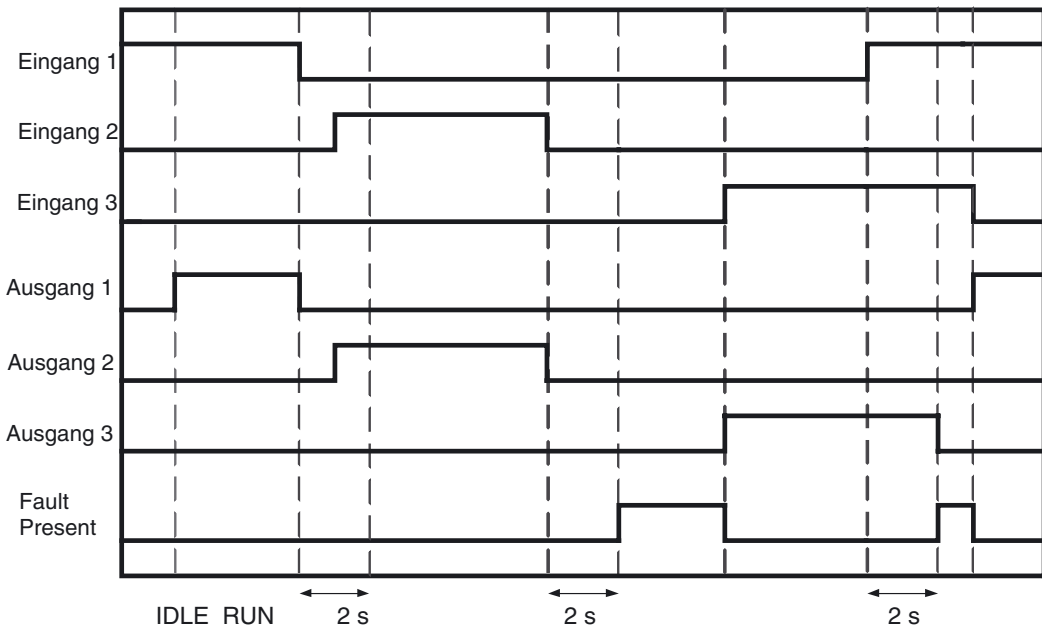
0: AUS, 1: EIN

Fehlerbehandlung und Zurücksetzen des Fehlerzustands

Fehlerzustand	Verhalten bei Fehlererkennung		Zurücksetzen des Fehlerzustands
	Ausgänge	Fault Present	
Für einen Zeitraum von mehr als zwei Sekunden war mehr als ein Eingang auf EIN gesetzt.	AUS (Sicherheitszustand)	EIN	Beseitigen Sie die Fehlerursache. (Korrigieren Sie das System so, dass immer nur ein Kontakt auf EIN gesetzt ist.)
Für einen Zeitraum von mehr als zwei Sekunden waren alle Eingänge auf AUS gesetzt.			

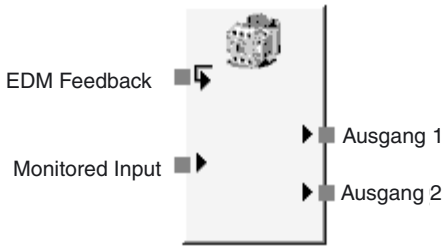
Hinweis Sind zwei oder mehr Eingänge gleichzeitig auf EIN gesetzt, wird der dem ersten Eingang entsprechende Ausgang für zwei Sekunden auf EIN gesetzt. Wenn mehrere Eingänge im selben Zyklus des Sicherheitsnetzwerk-Controllers NE1A aktiviert werden (EIN), werden alle Ausgänge auf AUS gesetzt sind.

Zeitablaufdiagramm



6-5-10 Funktionsblock: Externe Relaisüberwachung

Diagramm



Standardbelegung (Ein- und Ausgänge)

Allgemeine Beschreibung

Der Funktionsblock für die externe Relaisüberwachung überwacht das Eingangssignal und den Ausgangszustand eines externen Relais. Dazu stellt der Funktionsblock Sicherheitsausgänge für das externe Relais zur Verfügung.

Wird das Eingangssignal „Monitored Input“ auf EIN gesetzt, werden die Ausgangssignale 1 und 2 auf EIN gesetzt. In diesem Fall muss sich der Zustand des Rückführungssignals innerhalb der festgelegten Zeitspanne ändern. Wird das Eingangssignal „Monitored Input“ auf AUS gesetzt, werden die Ausgangssignale 1 und 2 auf AUS gesetzt. In diesem Fall muss sich der Zustand des Rückführungssignals innerhalb der festgelegten Zeitspanne ändern.

Erfolgt diese Zustandsänderung nicht innerhalb der festgelegten Zeitspanne, tritt ein EDM-Fehler auf. In diesem Fall werden die Ausgangssignale 1 und 2 auf AUS und das Signal „EDM Error“ auf EIN gesetzt.

Parametereinstellungen

Einstellung	Einstellbereich	Standardeinstellung
EDM Feedback Maximum Time Delay (T_{EDM})	100 bis 1000 ms (in 10-ms-Schritten)	300 ms

Die Einstellung des Parameters „EDM Feedback Maximum Time Delay“ muss größer sein als die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A.

Bei der Übernahme des Rückführungssignals eines abgesetzten Geräts muss die Netzwerkantwortzeit mit berücksichtigt werden.

Optionale Ausgangseinstellungen

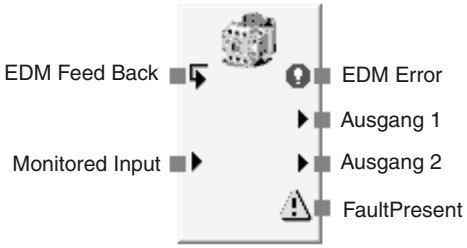
Bei der Programmierung können auch die folgenden Ausgänge genutzt werden. Um einen dieser optionalen Ausgänge zu aktivieren, muss das Kontrollkästchen auf der Registerkarte „Out Point“ des Eigenschaftendialogfelds des Funktionsblocks aktiviert werden.

EDM Error

Ausgang 2

Einstellung „Use Fault Present“

Bei der Programmierung kann auch der Ausgang „Fault Present“ genutzt werden. Damit dieser optionale Ausgang im Logik-Editor angezeigt wird, muss das Kontrollkästchen „Fault Present“ auf der Registerkarte „Out Point“ des Eigenschaftendialogfelds des Funktionsblocks aktiviert werden.

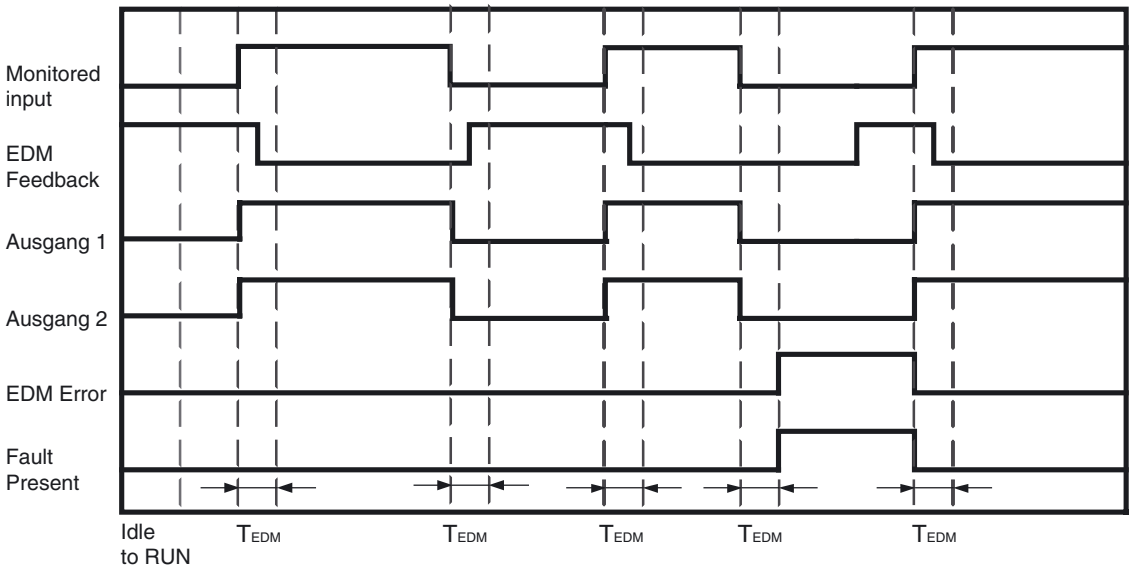


Funktionsblock für die externe Relaisüberwachung mit maximaler Eingangs- und Ausgangszahl

Fehlerbehandlung und Zurücksetzen des Fehlerzustands

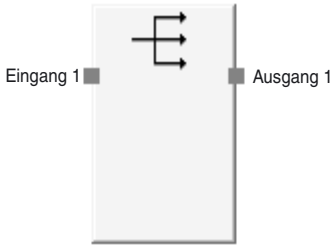
Fehler-zustands	Verhalten bei Fehlererkennung			Zurücksetzen des Fehlerzustand
	Ausgänge 1 und 2	Fault Present	Fehlerausgang	
EDM-Rückführung-Zeitüberschreitungsfehler	AUS (Sicherheitszustand)	EIN	Ausgang „EDM Error“: EIN	Beheben Sie die Ursache des Fehlers, und setzen Sie den Sicherheitseingang auf EIN.

Zeitablaufdiagramm



6-5-11 Logikfunktion: Routing

Diagramm



Standardbelegung (Ein- und Ausgänge)

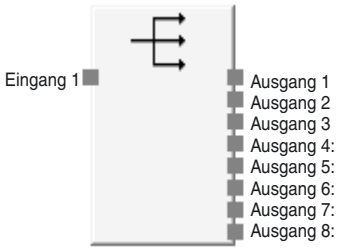
Allgemeine Beschreibung

Die Logikfunktion „Routing“ verteilt ein Eingangssignal auf bis zu acht Ausgangssignale. Sie ermöglicht die Ausgabe eines Signals an mehrerer Ausgabe-Tags.

Optionale Ausgangseinstellungen

Die Anzahl der Ausgänge kann auf der Registerkarte „In/Out Setting“ des Eigenschaftendialogfelds der Logikfunktion auf einen Wert zwischen 1 und 8 eingestellt werden.

Einstellung	Einstellbereich	Standardeinstellung
Number of Outputs	1 bis 8	1



Logikfunktion „Routing“ mit der maximal möglichen Zahl von Ausgängen

Wahrheitstabelle

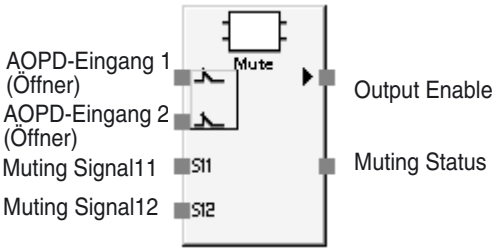
Wahrheitstabelle für die Logikfunktion „Routing“

Eingang 1	Ausgang 1	Ausgang 2	Ausgang 3	Ausgang 4	Ausgang 5	Ausgang 6	Ausgang 7	Ausgang 8
0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1

0: AUS, 1: EIN

6-5-12 Funktionsblock: Muting

Diagramm



Standardbelegung (Ein- und Ausgänge)

Allgemeine Beschreibung

Diese Funktion steht nur beim Sicherheitsnetzwerk-Controller NE1A ab Geräteversion 1.0 zur Verfügung.

Der Funktionsblock „Muting“ deaktiviert vorübergehend das Lichtunterbrechungssignal (AOPD-Eingang) eines Lichtgitters, solange das Muting-Signal erkannt wird. Bei aktivierter Muting-Funktion können Schaltobjekte aus dem Erfassungsbereich entnommen werden, ohne dass die Maschine angehalten wird.

Außerdem besitzt der Funktionsblock „Muting“ eine Override-Funktion zur erzwungenen Aktivierung (EIN) des Signals „Output Enable“, ohne dass die Voraussetzungen für die Muting-Funktion erfüllt sein müssen. (Beispielsweise können mit der Maschine Objekte aus dem Erfassungsbereich des Lichtgitters beseitigt werden, die dort liegengeblieben sind.)

Die vier folgenden Muting-Funktionen stehen zur Auswahl.

Muting-Modus	Anwendung
Paralleles Muting mit 2 Sensoren	Eignet sich für den Einsatz im Eingangsbereich von Förderanlagen. Verwenden Sie diese Variante zusammen mit zwei Reflexionslichtschranken, die als Muting-Sensoren mit überlappenden Erfassungsbereichen fungieren.
Sequentielles Muting (vorwärts)	Eignet sich für den Einsatz im Eingangsbereich von Förderanlagen. Verwenden Sie diese Variante zusammen mit vier Einweglichtschranken, die als Muting-Sensoren fungieren.
Sequentielles Muting (bidirektional)	Eignet sich für den Einsatz im Ein- und Ausgangsbereich von Förderanlagen. Verwenden Sie diese Variante zusammen mit vier Einweglichtschranken, die als Muting-Sensoren fungieren.
Positionserkennung	Eignet sich für Einsatzbereiche, in denen das Muting über einen Schaltereingang gesteuert wird.

Hinweis Die obige Erläuterung geht davon aus, dass die Muting-Sensoren auf EIN gesetzt sind, wenn eine Erfassung stattfindet, während sie auf AUS gesetzt sind, wenn keine Erfassung stattfindet.

Parametereinstellungen

Einstellung	Einstellbereich	Standard-einstellung
Input Type (Lichtgitterausgang)	• Dual Channel Equivalent (Öffner/Öffner) • Dual Channel Complementary (Öffner/Schließer)	Dual Channel Equivalent
Diskrepanzzeit (Lichtgitterausgang)	10 bis 500 ms (in 10-ms-Schritten) (siehe Hinweis) Bei der Einstellung 0 erfolgt keine Überprüfung der Diskrepanzzeit.	30 ms
Input Type (Override-Signal)	• Single Channel • Dual Channel Equivalent (Schließer/Schließer) • Dual Channel Complementary (Öffner/Schließer) • Nicht verwendet.	Nicht verwendet.
Discrepancy Time (Override-Signal)	10 bis 500 ms (in 10-ms-Schritten) (siehe Hinweis) Bei der Einstellung 0 erfolgt keine Überprüfung der Diskrepanzzeit.	30 ms
Max. Override Time	500 ms bis 127,5 s (in 500-ms-Schritten)	60 s
Muting Mode	Positionserkennung Paralleles Muting mit 2 Sensoren Sequentielles Muting (vorwärts) Sequentielles Muting (bidirektional)	Paralleles Muting mit 2 Sensoren
Max Muting Time	500 ms bis 127,5 s (in 500-ms-Schritten) 0 bis 500 ms (in 10-ms-Schritten) Die Muting-Zeit ist unendlich, wenn „0“ eingestellt wird.	60 s
Synchronization Time (zwischen Muting-Signal 11 und Muting-Signal 12 oder zwischen Muting-Signal 21 und Muting-Signal 22)	30 ms bis 3 s (in 10-ms-Schritten) (siehe Hinweis)	3 s

Hinweis Der Zeitsollwert muss größer sein die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A.

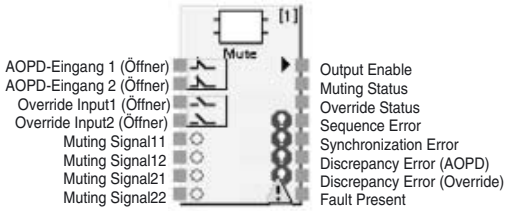
Optionale Ausgangseinstellungen

Bei der Programmierung können auch die folgenden Ausgänge genutzt werden. Damit diese optionalen Ausgänge aktiviert werden, muss die Anzahl der Ausgänge auf der Registerkarte „In/Out Setting“ des Eigenschaftenfelds des Funktionsblocks erhöht werden.

- Override Status
- Synchronization Error
- Sequence Error
- Discrepancy Error (AOPD)
- Discrepancy Error (Override)

Einstellung „Use Fault Present“

Bei der Programmierung kann auch der Ausgang „Fault Present“ genutzt werden. Damit dieser optionale Ausgang im Logik-Editor angezeigt wird, muss das Kontrollkästchen „Fault Present“ auf der Registerkarte „In/Out Setting“ des Eigenschaftendialogfelds des Funktionsblocks aktiviert werden.



Maximale Anzahl E/A-Punkte für einen Muting-Funktionsblock

Fehlerbehandlung und Zurücksetzen des Fehlerzustands

Fehlerzustand	Verhalten bei Fehlererkennung			Zurücksetzen des Fehlerzustands
	Output Enable	Fault Present	Fehlerausgang	
Synchronization Error (Zwischen Muting-Signal 11 und Muting-Signal 12) (Zwischen Muting-Signal 21 und Muting-Signal 22) (siehe Hinweis 1)	EIN (Siehe Hinweis 3)	AUS (Siehe Hinweis 3)	Synchronisationsfehler: EIN	Reset erfolgt bei erneutem Muting oder wenn der Betriebsmodus des Sicherheitsnetzwerk-Controllers NE1A zu IDLE und wieder zurück zu RUN geschaltet wird.
Sequence Error			Sequenzfehler: EIN	
Discrepancy Error (AOPD)	AUS (Sicherheitszustand)	EIN	Diskrepanzfehler (AOPD): EIN	Beide Lichtgitter-Eingangssignale wechseln von inaktiv zu aktiv, oder der Betriebsmodus des Sicherheitsnetzwerk-Controllers wechselt zu IDLE und dann wieder zurück zu RUN.
Discrepancy Error (Override)			Diskrepanzfehler (Override): EIN	Beide Override-Eingangssignale wechseln von inaktiv zu aktiv, oder der Betriebsmodus des Sicherheitsnetzwerk-Controllers wechselt zu IDLE und dann wieder zurück zu RUN.

Hinweis

(1) Wird nur erkannt, wenn *Sequential Muting (bidirektional)* eingestellt ist.

(2) Wenn mehrere Fehler auftreten, werden Fehler an allen Fehlerausgängen angezeigt.

(3) Wenn das Lichtgitter von diesem Fehlerstatus zu inaktiv (kein Licht) wechselt, wird das Signal „Output Enable“ auf AUS gesetzt, während das Signal „Fault Present“ auf EIN gesetzt wird. Wenn das Lichtgitter aktiviert (Lichteinfall) oder die Override-Funktion ausgeführt wird, wird das Signal

„Output Enable“ auf EIN gesetzt, während das Signal „Fault Present“ auf AUS gesetzt wird.

Muting-Funktion

Muting: Start- und Stopp-Bedingungen

■ Rücksetzbedingungen

„Output Enable“ ist EIN, wenn alle folgenden Voraussetzungen erfüllt werden.

- Das Lichtgittersignal ist aktiv (Lichteinfall).
- Es ist kein Diskrepanzfehler aufgetreten.

■ Start-Bedingungen

Wenn die Muting-Signale die folgenden Voraussetzungen erfüllen, während das Signal „Output Enable“ EIN lautet, erfolgt das Muting und „Muting Status“ wird auf EIN gesetzt.

1. Alle Muting-Sensoren sind AUS.
2. Während alle Muting-Sensoren AUS sind, werden zwei Muting-Signale in der richtigen Reihenfolge erkannt.
3. Während alle Muting-Sensoren AUS sind, liegen die Synchronisationszeiten der beiden Muting-Signale innerhalb des Normalbereichs (ohne Positionserkennung).

Wenn einer der oben aufgeführten Fehler auftritt, werden die folgenden Alarmausgänge generiert.

- Das Signal „Sequence Error“ wird auf EIN gesetzt, falls eine ungültige Reihenfolge vorliegt (siehe oben).
- Das Signal „Synchronization Error“ wird auf EIN gesetzt, wenn innerhalb der Synchronisierungszeit kein Objekt erfasst werden kann (siehe oben).

Außerdem wird der Sicherheitsausgang auf AUS gesetzt, wenn das Lichtgittersignal inaktiv ist (kein Licht), bevor der Controller in den Muting-Zustand wechselt.

■ Stoppbedingungen

Wenn die folgenden Voraussetzungen erfüllt werden, während das Muting erfolgt, wird das Muting gestoppt und der Muting-Status wechselt zu AUS.

- Mindestens zwei Muting-Signale lauten nicht EIN.
- Die max. Muting-Zeit ist abgelaufen.
- Es ist ein Diskrepanzfehler aufgetreten.

Außerdem wechselt das Signal „Output Enable“ zu AUS, wenn das Muting gestoppt wird und das Lichtgitter blockiert ist.

Hinweis Wenn der Betriebsmodus des Sicherheitsnetzwerk-Controllers NE1A von „Idle“ zu „Run“ umgeschaltet wird, werden die Eingangsdaten von den Slaves auf AUS gesetzt, bis die Kommunikation hergestellt ist.
Wenn Slave-Eingangsdaten für den AOPD-Eingang verwendet werden, werden die Ausgänge „Fault Present“ und „Sequence Error“ auf EIN gesetzt, sobald der Betriebsmodus zu „Run“ gewechselt hat. Wenn der AOPD-Eingang zu EIN wechselt, wird der Ausgang „Fault Present“ auf AUS gesetzt. Wenn die Muting-Startbedingungen erfüllt sind, wird der Ausgang „Sequence Error“ auf AUS gesetzt.

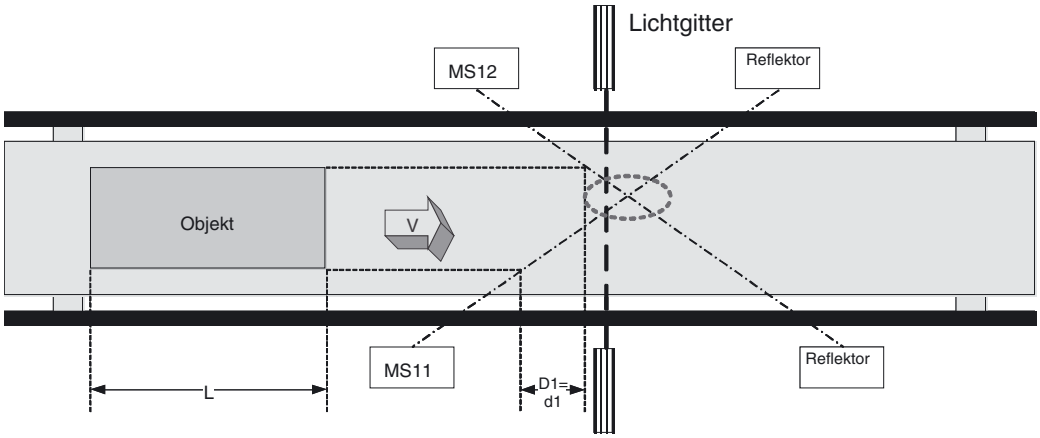
Beispiele für Muting-Systemkonfigurationen

■ Paralleles Muting mit 2 Sensoren

In diesem Beispiel werden zwei Reflexionslichtschranken als Muting-Sensoren mit überlappenden Erfassungsbereichen konfiguriert.

Verwenden Sie diese Konfiguration, wenn die Objektlänge (L) nicht fest oder nicht lang genug ist.

Blockschaltbild



MS11: Mit Muting-Signal 11 verbundener Muting-Sensor

MS12: Mit Muting-Signal 12 verbundener Muting-Sensor

Hinweis Der Schnittpunkt der beiden Sensoren muss hinter dem Lichtgitter liegen.

Muting-Sequenz

1. Im obigen Blockschaltbild ist das Licht zwischen MS11 und MS12 und Lichtgitter nicht unterbrochen. Daher lautet das Output-Enable-Signal EIN.
2. Während sich das Objekt nach rechts bewegt und MS11 und MS12 nacheinander zu EIN wechseln, wir das Muting aktiviert.
3. Während sich das Objekt weiterbewegt, bleibt das Output-Enable-Signal auch dann aktiviert (EIN), wenn das Lichtgitter blockiert wird.
4. Wenn sich das Objekt noch weiter bewegt, wird das Licht von MS11 nicht mehr vom Objekt unterbrochen, der Muting-Status wird aufgehoben und „Muting Status“ wechselt zu AUS.

Konfigurationsabstände

Die nachstehende Formel bezeichnet den für eine wirkungsvolle Muting-Funktion der Muting-Sensoren erforderlichen Mindestabstand D1 :

Formel 1: $D1 < L$

L: Länge des Objekts

Die nachstehende Formel bezeichnet den für eine wirkungsvolle Muting-Funktion der Muting-Sensoren erforderlichen Höchstabstand d1 :

Formel 2: $V \times T1min < d1 < V \times T1max$

V: Durchgangsgeschwindigkeit des Objekts

T1min: Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A

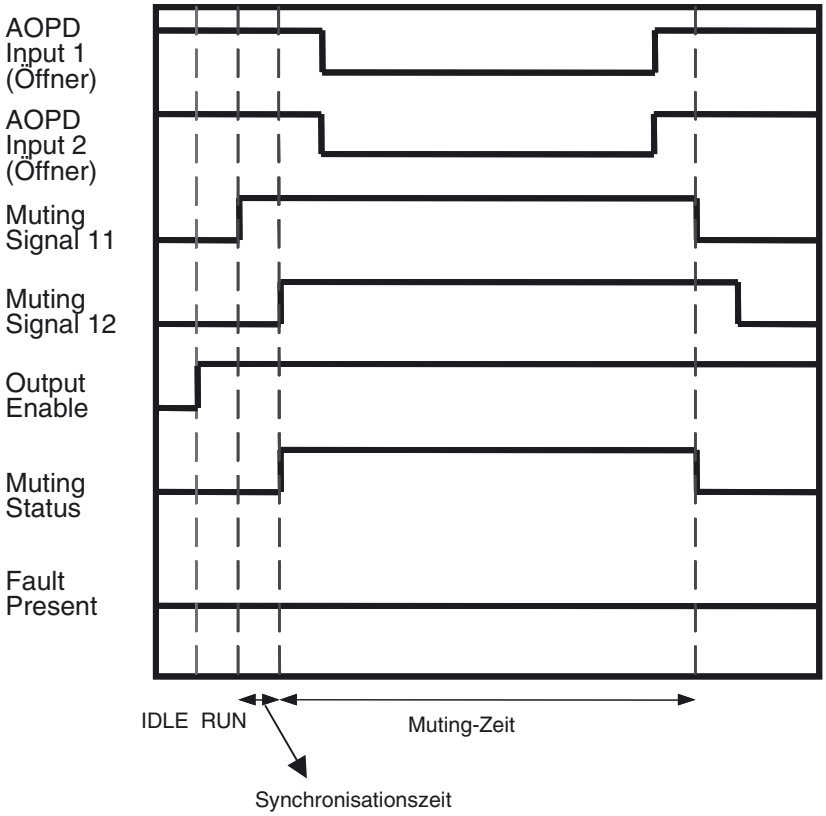
T1max: konfigurierte Synchronisationszeit

Die Standardeinstellung beträgt 3 s.

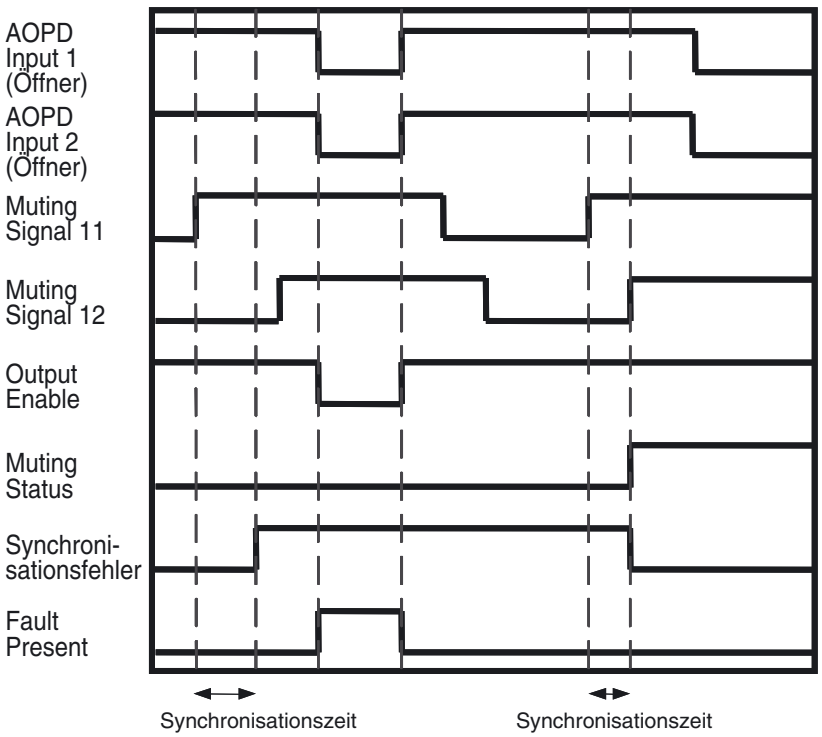
D1 muss Formel 1 und d1 Formel 2 genügen, damit die Muting-Funktion wirksam funktioniert. Diese Abstände müssen verhindern, dass eine vorbeigehende Person die Muting-Funktion aktivieren kann. Außerdem müssen Lichtgitter und Muting-Sensoren so konfiguriert werden, dass ein Objekt bereits alle Muting-Sensoren passiert hat, bevor nach nächste Objekt die Muting-Sensoren erreicht.

■ **Zeitablaufdiagramm**

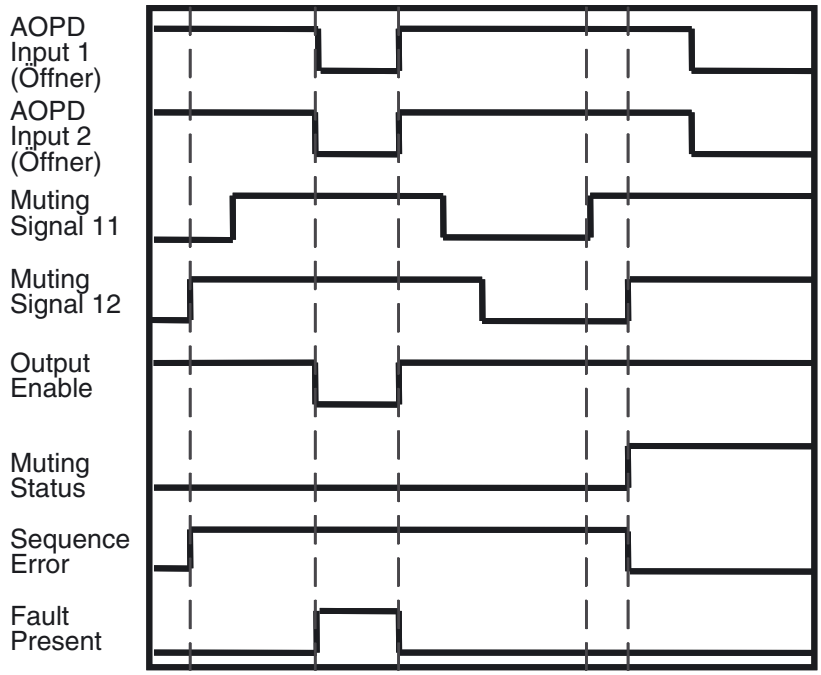
Normaler Betrieb



Synchronization Error



Sequence Error

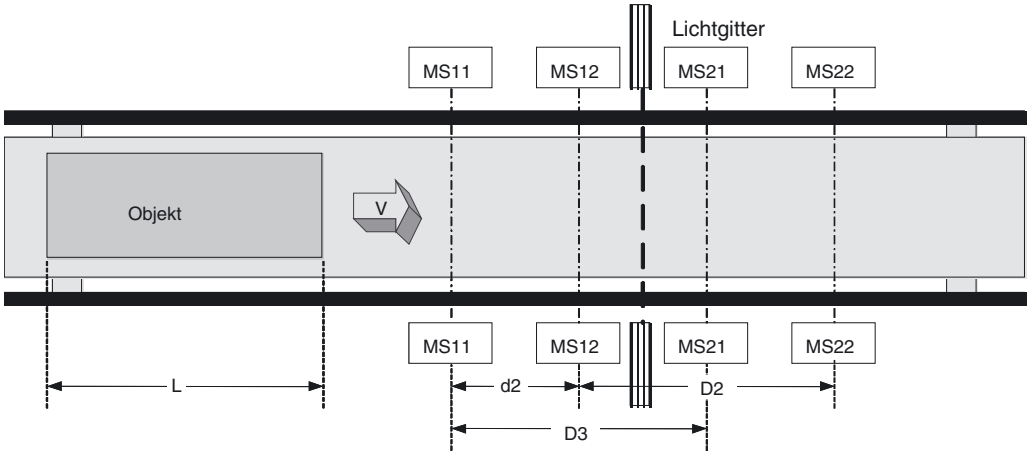


■ Sequentielles Muting (vorwärts)

In diesem Beispiel werden vier Einweglichtschranken als Sensoren mit überlappenden Erfassungsbereichen konfiguriert.

Verwenden Sie diese Konfiguration, wenn die Länge des transportierten Objekts größer ist als eine feste Länge.

Blockschaltbild



MS11: Mit Muting-Signal 11 verbundener Muting-Sensor

MS12: Mit Muting-Signal 12 verbundener Muting-Sensor

MS21: Mit Muting-Signal 21 verbundener Muting-Sensor

MS22: Mit Muting-Signal 22 verbundener Muting-Sensor

Muting-Sequenz

1. Im obigen Blockschaltbild ist das Licht zwischen MS11, MS12, MS21 und MS22 und Lichtgitter nicht unterbrochen. Daher lautet das Output-Enable-Signal EIN.
2. Während sich das Objekt nach rechts bewegt und MS11 und MS12 nacheinander auf EIN gesetzt werden, wird das Muting aktiviert und der Muting-Status wechselt zu EIN.
3. Während sich das Objekt weiterbewegt, bleibt das Output-Enable-Signal auch dann aktiviert (EIN), wenn das Lichtgitter blockiert wird.
4. Wenn sich das Objekt noch weiter bewegt, wird das Licht von MS21 nicht mehr vom Objekt unterbrochen, der Muting-Status wird aufgehoben und „Muting Status“ wechselt zu AUS.

Konfigurationsabstände

Die nachstehenden Formeln bezeichnen die für eine wirkungsvolle Muting-Funktion der Muting-Sensoren erforderlichen Mindestabstände D2 und D3:

Formel 3: $D2 < L$

Formel 4: $D3 < L$

L: Länge des Objekts

Die nachstehende Formel bezeichnet den für eine wirkungsvolle Muting-Funktion der Muting-Sensoren erforderlichen Höchstabstand d2:

Formel 5: $V \times T1min < d2 < V \times T1max$

V: Durchgangsgeschwindigkeit des Objekts

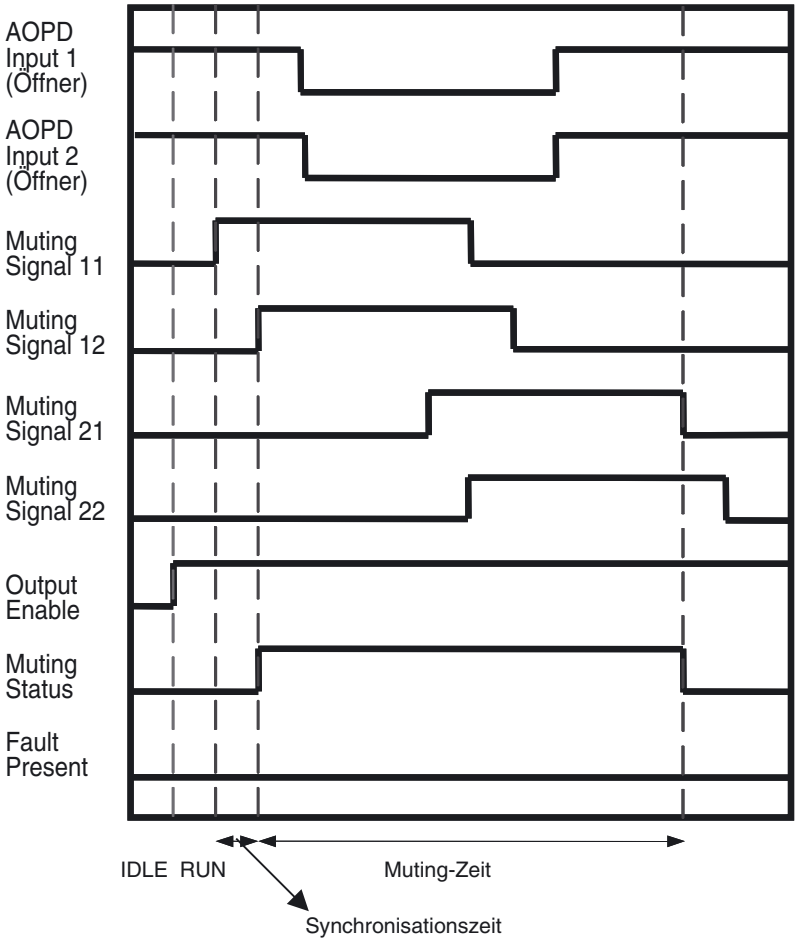
T1min: Zykluszeit des Sicherheitsnetzwerk-Controllers NEA1

T1max: Synchronisationszeit

Die Standardeinstellung beträgt 3 s.

D2 muss Formel 1 genügen, D3 muss Formel 4 genügen, und d5 muss Formel 5 genügen, damit die Muting-Funktion wirksam funktioniert. Diese Abstände müssen verhindern, dass eine vorbeigehende Person die Muting-Funktion aktivieren kann. Außerdem müssen Lichtgitter und Muting-Sensoren so konfiguriert werden, dass ein Objekt bereits alle Muting-Sensoren passiert hat, bevor nach nächste Objekt die Muting-Sensoren erreicht.

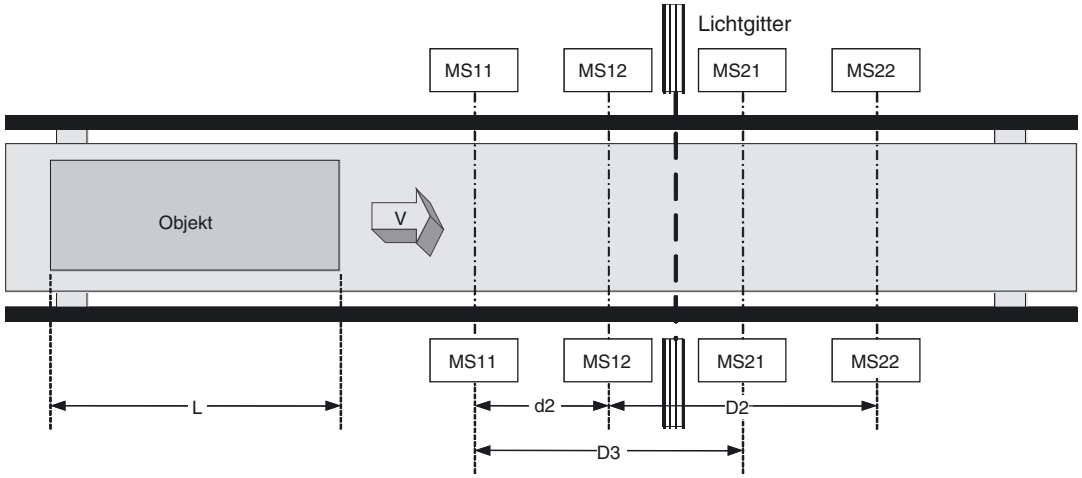
■ **Zeitablaufdiagramm**



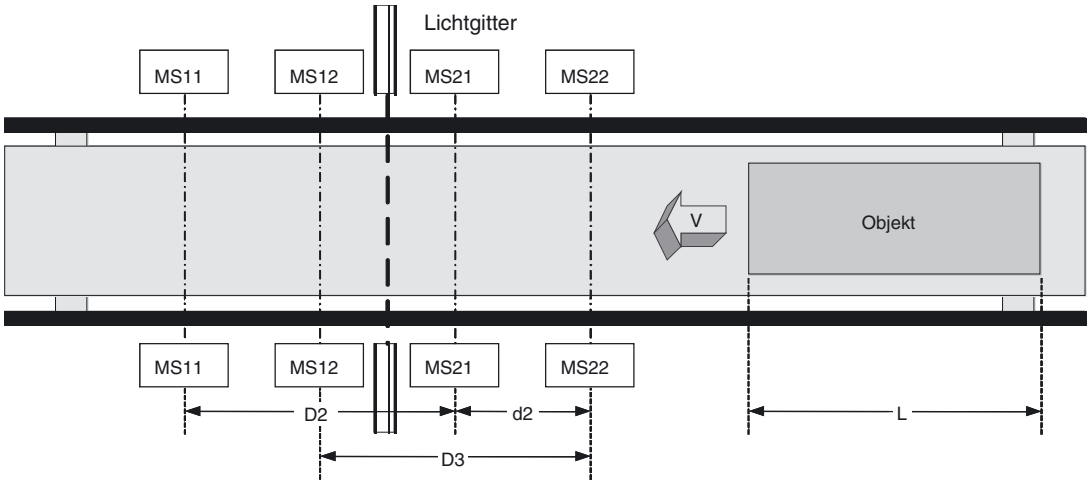
■ **Sequentielles Muting (bidirektional)**

Blockschaltbild

1. Eingang



2. Ausgang



MS11: Mit Muting-Signal 11 verbundener Muting-Sensor

MS12: Mit Muting-Signal 12 verbundener Muting-Sensor

MS21: Mit Muting-Signal 21 verbundener Muting-Sensor

MS22: Mit Muting-Signal 22 verbundener Muting-Sensor

Muting-Sequenz

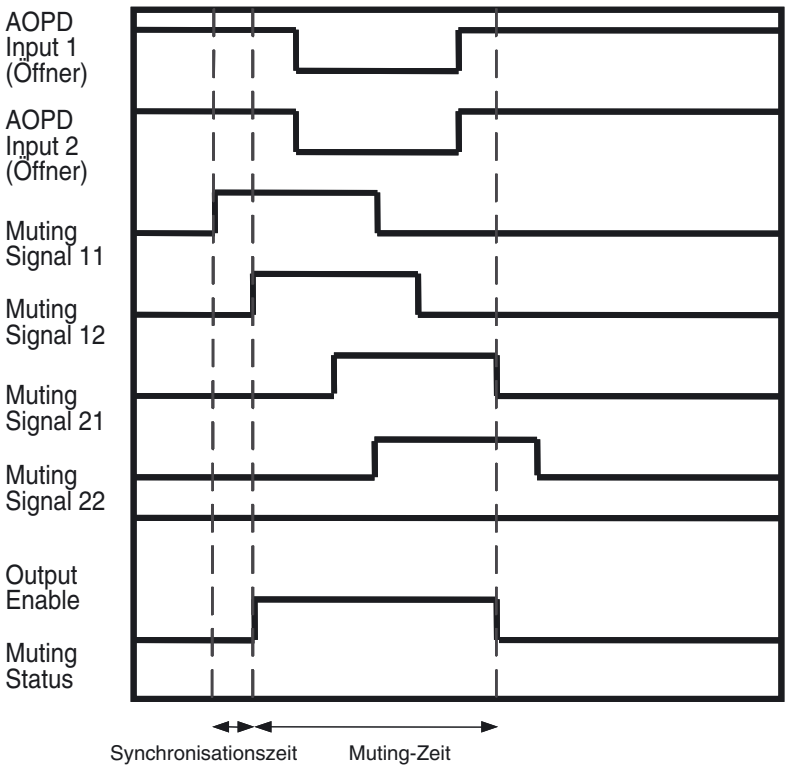
1. Im obigen Blockschaltbild ist das Licht zwischen MS11, MS12, MS21 und MS22 und Lichtgitter nicht unterbrochen. Daher lautet das Output-Enable-Signal EIN.
2. Während sich das Objekt im Eingangsbereich nach rechts bewegt und MS11 und MS12 nacheinander auf EIN gesetzt werden (am Ausgang wechseln MS22 und MS21 zu EIN), wird das Muting aktiviert und „Muting Status“ wechselt zu EIN.
3. Während sich das Objekt weiterbewegt, bleibt das Output-Enable-Signal auch dann aktiviert (EIN), wenn das Lichtgitter blockiert wird.
4. Wenn sich das Objekt noch weiter bewegt, wird es nicht mehr von MS21 am Eingang (am Ausgang: MS12) erkannt, der Muting-Status wird aufgehoben und „Muting Status“ wechselt zu AUS.

Konfigurationsabstände

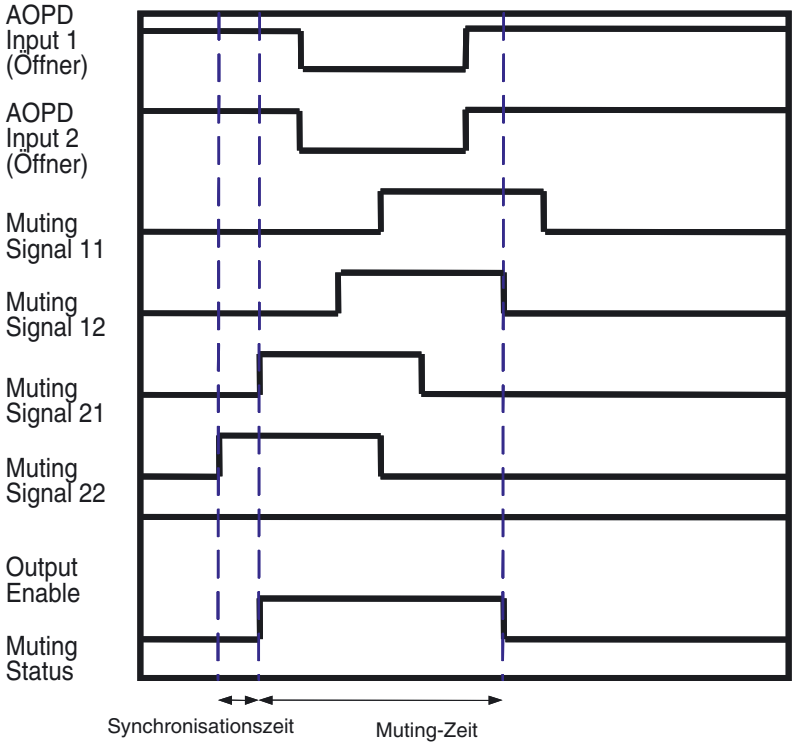
Die erforderlichen Konfigurationsabstände sind mit denen für *Sequentielles Muting (Vorwärts)* identisch.

■ Zeitablaufdiagramm

Eingang



Zeitdifferenz Eingangsmuster 2: Ausgang

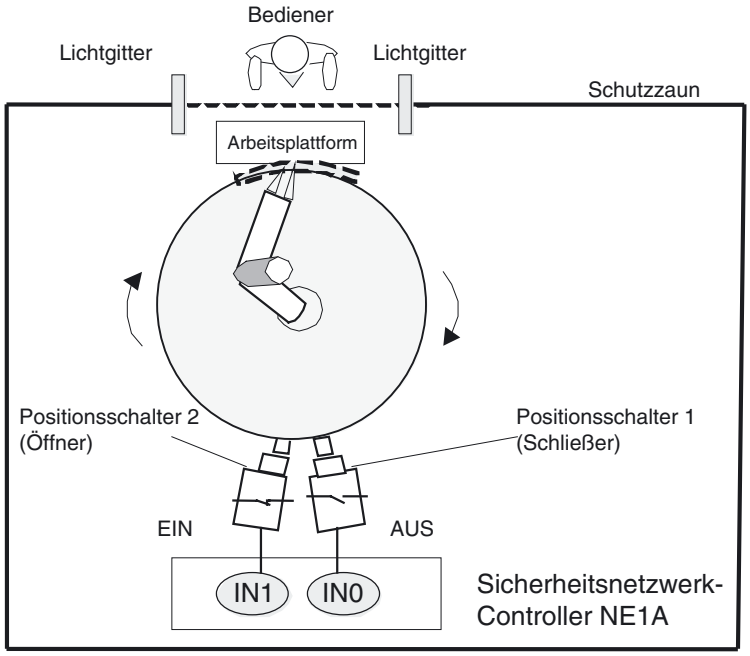


■ Positionserkennung

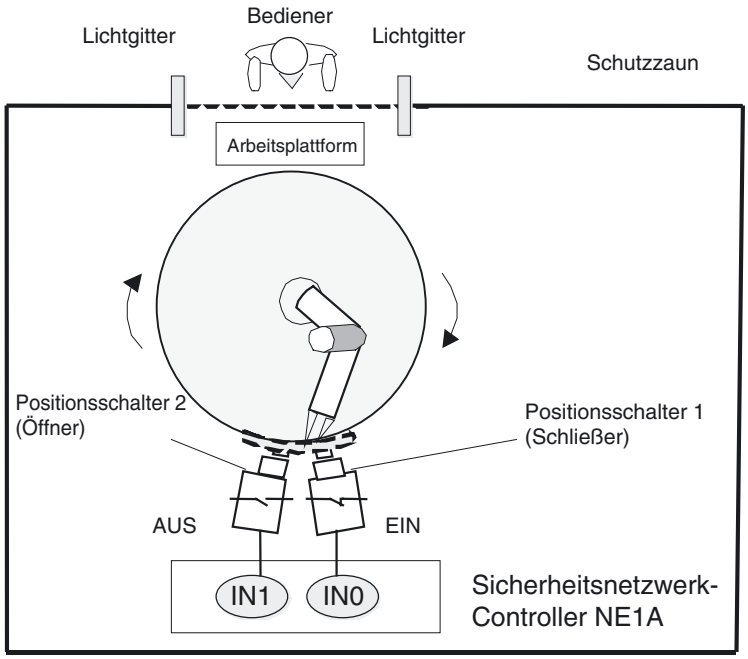
In diesem Anwendungsbeispiel befindet sich das Objekt auf einem Drehtisch, der von einem Schutzzaun umgeben ist. Der Bediener kann das Lichtunterbrechungssignal des Sicherheitslichtgitters deaktivieren, um ein Objekt auf dem Drehtisch zu positionieren, wenn er sich gegenüber dem Gefahrenbereich der Maschine aufhält.

Blockschaltbild

Gefahrenbereich der Maschine auf der Seite des Bedieners (Abbildung 1):



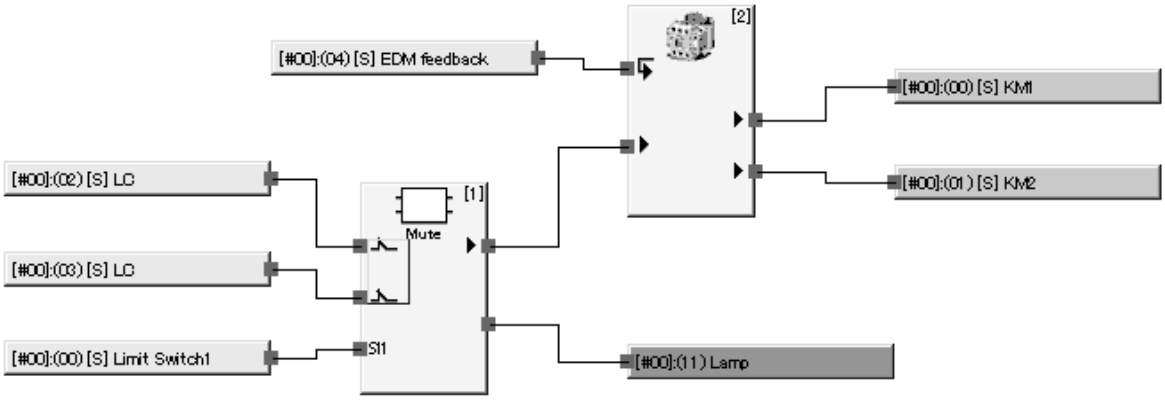
Gefahrenbereich der Maschine auf der gegenüberliegenden Seite des Bedieners (Abbildung 2):



Hinweis Konfigurieren Sie den Zweikanalmodus für lokale Eingänge des Sicherheitsnetzwerk-Controllers NEA1 als Zweikanal-Komplementärmodus.

Programmbeispiel

Die Positionsschalter 1 und 2 sind über eine AND-Funktion mit dem Muting-Signal 11 des Muting-Funktionsblocks verbunden.

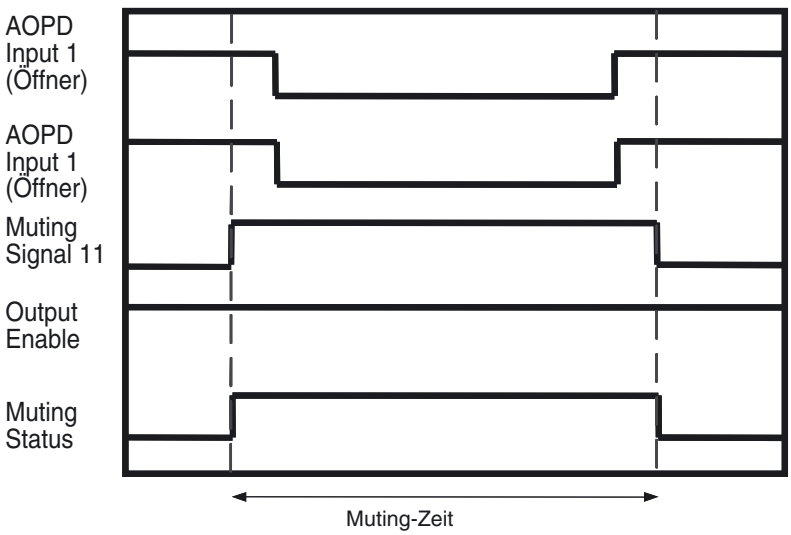


Hinweis Die Positionsschalter 1 und 2 sind als Zweikanal-komplementär konfiguriert, damit die lokalen Eingänge die Eingangsdaten der beiden Schalter analysieren können.

Muting-Sequenz

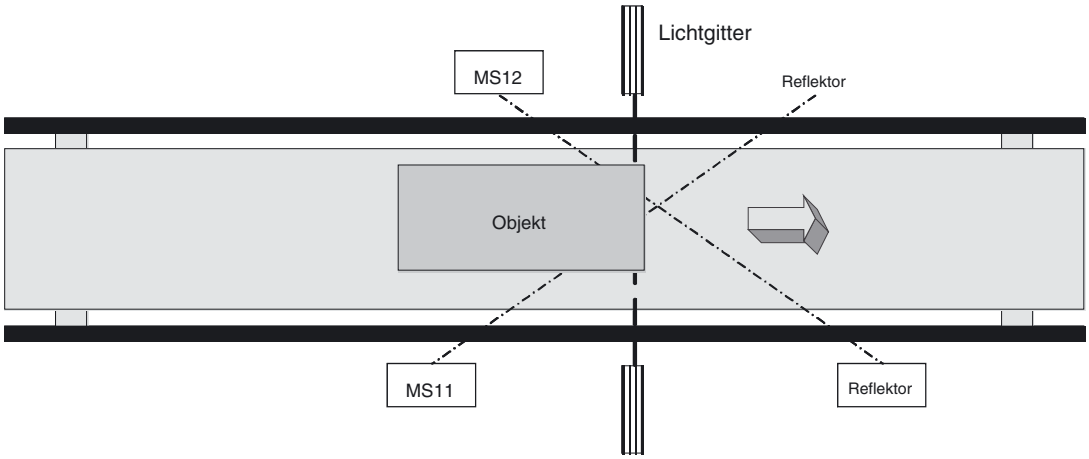
1. Im obigen Beispiel ist Positionsschalter 1 (Schließer) AUS, während Positionsschalter 2 (Öffner) EIN ist.
   Außerdem ist das Lichtgitter nicht blockiert, daher lautet das Output-Enable-Signal „EIN“. Muting Signal 11 (zur Übermittlung des Zweikanal-Komplementärsignals für die Positionsschalter 1 und 2) wechselt zu AUS.
2. Während sich der Roboterarm dreht, wechselt Positionsschalter 1 zu EIN, während Positionsschalter 2 zu AUS wechselt (siehe Abbildung 2). Muting Signal 11 (zur Übermittlung des Zweikanal-Komplementärsignals für die Positionsschalter 1 und 2) wechselt zu EIN, das Muting wird aktiviert, und „Muting Status“ wechselt zu EIN.
3. Zu diesem Zeitpunkt wird das Signal „Output Enable“ auch dann auf EIN gehalten, wenn das Lichtgitter
   blockiert ist, damit der Bediener Zugang zur Arbeitsplattform erhält.
4. Wenn der Bediener seine Arbeit beendet hat und das Lichtgitter nicht mehr blockiert ist, da sich der Roboterarm weiterdreht, wechselt das Muting-Signal 11 zu AUS, der Muting-Status wird aufgehoben und „Muting Status“ wechselt zu AUS.

■ **Zeitablaufdiagramm**



Override-Funktion

Mit der Override-Funktion kann der Sicherheitsausgang auch dann auf EIN gesetzt werden, wenn das Lichtunterbrechungssignal des Lichtgitters inaktiv ist. Wenn ein Objekt während des Transports hängen bleibt (siehe Abbildung unten), kann das System nicht mehr in den normalen Betrieb zurückversetzt werden, ohne dass das Objekt mit Gewalt beseitigt wird. In diesem Fall kann die Override-Funktion dazu verwendet werden, das Objekt aus dem Erfassungsbereich des Lichtgitters zu transportieren.



MS11: Mit Muting-Signal 11 verbundener Muting-Sensor

MS12: Mit Muting-Signal 12 verbundener Muting-Sensor

Override-Sequenz

1. Im obigen Blockschaltbild ist das Signal „Output Enable“ AUS.
2. Wenn „Override Input“ zu EIN wechselt, beginnt die Override-Funktion und „Override Status“ wechselt zu EIN. Solange die Override-Eingänge auf EIN gesetzt sind, bleibt der Muting-Status zwangsweise aktiviert und die beiden Signale „Muting Status“ und „Output Enable“ sind EIN.
3. Wenn sich das Objekt nach rechts bewegt, bis es nicht mehr von MS12 erfasst wird, wird der mittels Override-Funktion erzwungene Muting-Status aufgehoben, und „Muting Status“ und „Override Status“ wechseln zu AUS.

■ Override: Start- und Stoppbedingungen

■ Start-Bedingungen

Wenn die folgenden Voraussetzungen erfüllt sind, beginnt die Override-Funktion und die Signale „Output Enable“, „Muting Status“ und „Override Status“ wechseln alle zu EIN.

1. Mindestens ein Muting-Signal ist auf EIN gesetzt.
2. Das Lichtgitter ist inaktiv (blockiert).
3. Das Signal „Output Enable“ ist auf AUS gesetzt.
4. „Override Input“ ist EIN (Einzelkonfiguration) oder „Active“ (Dualkonfiguration).

■ Stoppbedingungen

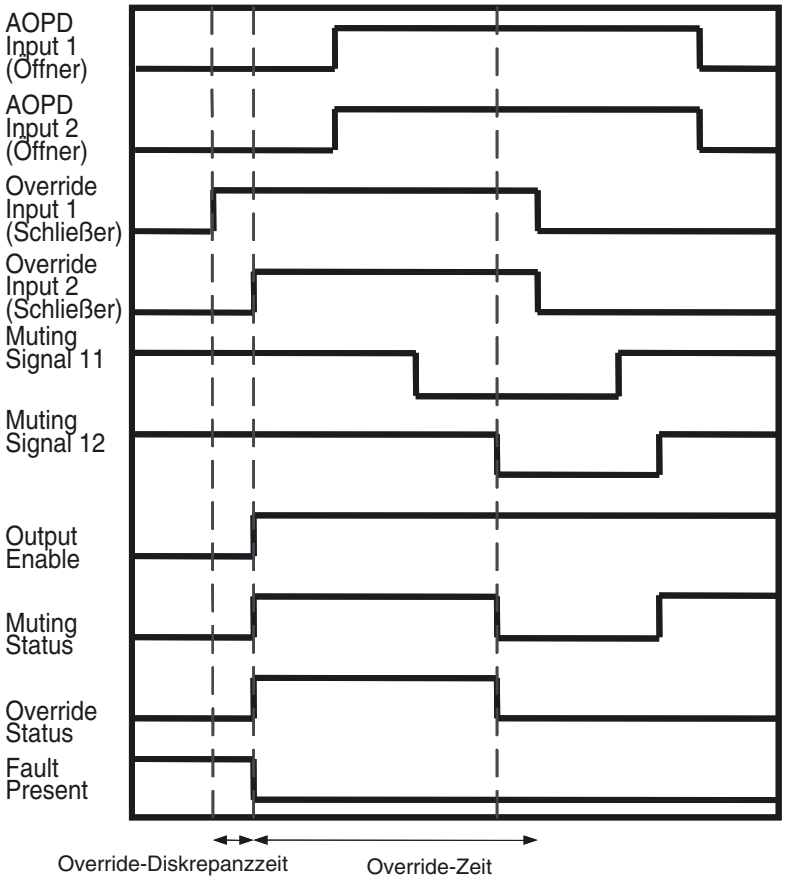
Wenn eine der folgenden Voraussetzungen erfüllt ist, stoppt die Override-Funktion und die Signale „Muting“ und „Overriding“ wechseln zu AUS.

1. Alle Muting-Signale sind AUS.
2. Die max. Override-Zeit ist abgelaufen.
3. „Override Input“ ist AUS (Einzelkonfiguration) oder „Inactive“ (Dualkonfiguration).

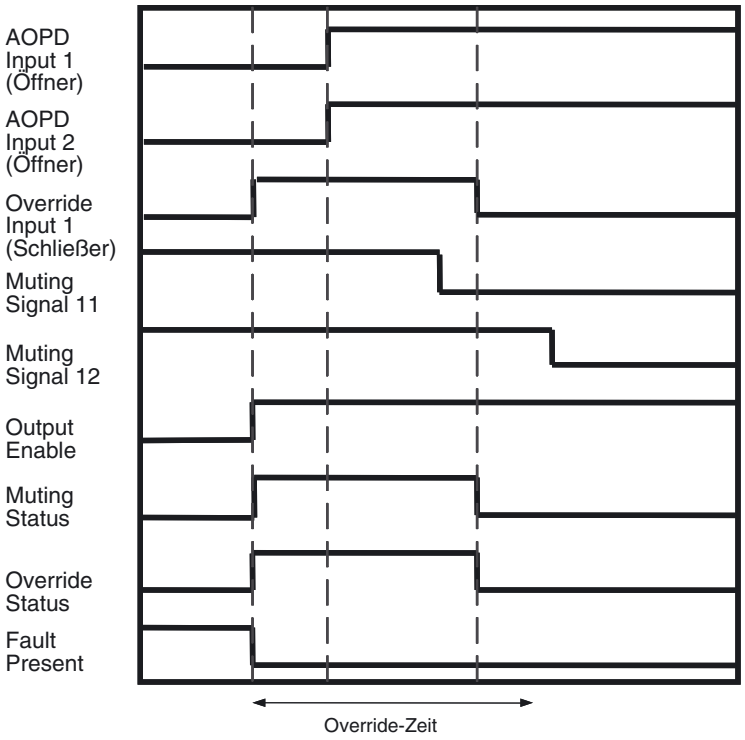
Nach Beendigung der Override-Funktion wechselt „Output Enable“ zu AUS, falls das Lichtgitter blockiert ist.

■ Zeitablaufdiagramm

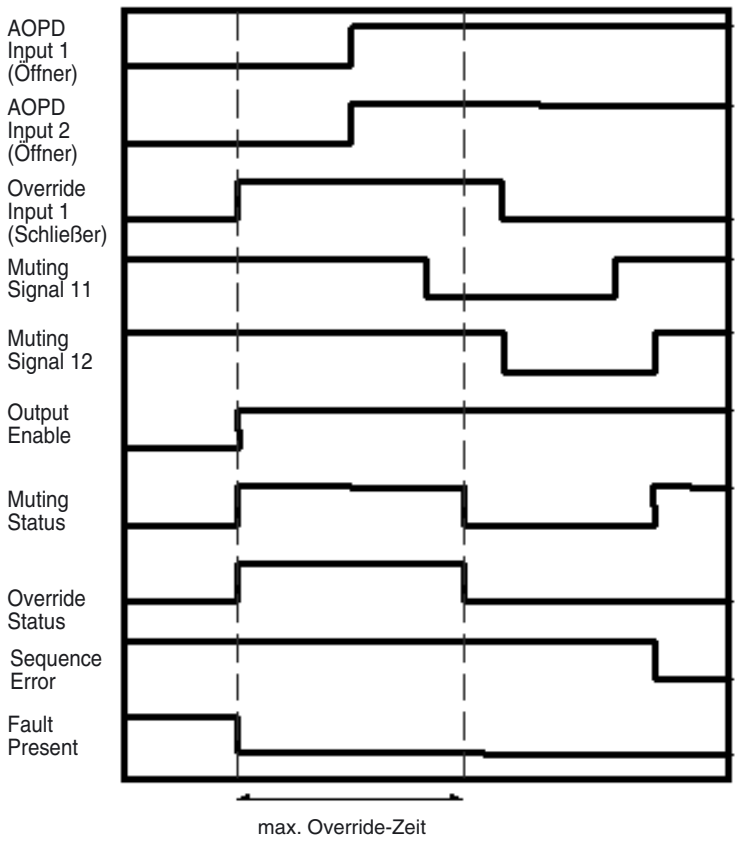
Normaler Betrieb der Override-Funktion (Muting-Modus: paralleles Muting mit 2 Sensoren)



Override-Signal wechselt beim Override zu AUS (Muting-Modus: Paralleles Muting mit 2 Sensoren)

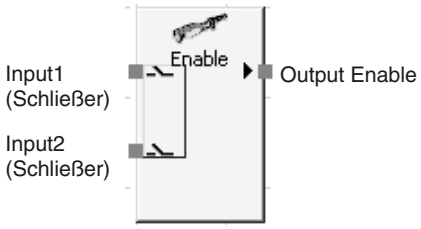


Override-Zeitüberschreitung beim Override (Muting-Modus: Paralleles Muting mit 2 Sensoren)



6-5-13 Funktionsblock: Zustimmschalterüberwachung

Diagramm



Standardbelegung (Ein- und Ausgänge)

Allgemeine Beschreibung

Diese Funktion steht nur beim Sicherheitsnetzwerk-Controller NE1A ab Geräteversion 1.0 zur Verfügung.

Der Funktionsblock „Enable Switch“ überwacht den Status des Zustimmschalters.

Der Ausgang „Output Enable“ ist EIN, wenn der Eingang des überwachten Zustimmschalters aktiv ist. Der Ausgang „Output Enable“ ist AUS, wenn der Eingang nicht aktiv ist oder innerhalb des Funktionsblocks ein Fehler festgestellt wird.

Wenn es sich um einen Zustimmschalter handelt, der ein Greif- und ein Freigabesignal ausgibt, kann außerdem der Status der Signale „Grip Input“ und „Release Input“ überwacht werden. Die empfangenen Signale „Grip Input“ und „Release Input“ haben keinen Einfluss auf den Status des Signals „Output Enable“.

Parametereinstellungen

Einstellung	Einstellbereich	Standard-einstellung
Input Type	Single Channel Dual Channel Equivalent	Dual Channel Equivalent
Diskrepanzzeit	0 bis 30 s (in 10-ms-Schritten) Bei der Einstellung 0 erfolgt keine Überprüfung der Diskrepanzzeit.	30 ms

Der Zeitsollwert muss größer sein die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A.

Anzahl der E/A-Punkte

Die Anzahl der Eingänge kann auf der Registerkarte „In/Out Setting“ des Eigenschaftendialogfelds der Logikfunktion auf einen Wert zwischen 1 und 8 eingestellt werden.

Einstellung	Einstellbereich	Standardeinstellung
Number of Inputs	2 bis 4 Es gibt auch dann zwei Eingänge, wenn *Input Type* in den Parametereinstellungen als *Single Channel* konfiguriert wurde. Die Signale „Grip Input“ und „Release Input“ können genutzt werden, wenn 3 oder 4 Eingänge konfiguriert sind.	2

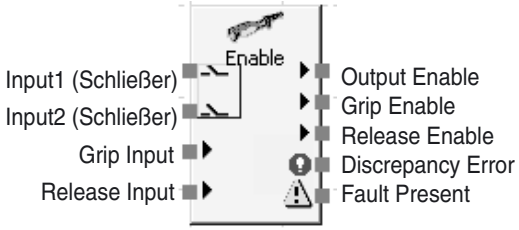
Optionaler Ausgang

Bei der Programmierung können auch die folgenden Ausgänge genutzt werden. Um einen dieser optionalen Ausgänge zu aktivieren, muss das entsprechende Kontrollkästchen auf der Registerkarte „Out Point“ des Eigenschaftendialogfelds des Funktionsblocks aktiviert werden.

- Grip Enable
- Release Enable
- Discrepancy Error

Einstellung „Use Fault Present“

Bei der Programmierung kann auch der Ausgang „Fault Present“ genutzt werden. Damit dieser optionale Ausgang im Logik-Editor angezeigt wird, muss das Kontrollkästchen „Fault Present“ auf der Registerkarte „Out Point“ des Eigenschaftendialogfelds des Funktionsblocks aktiviert werden.



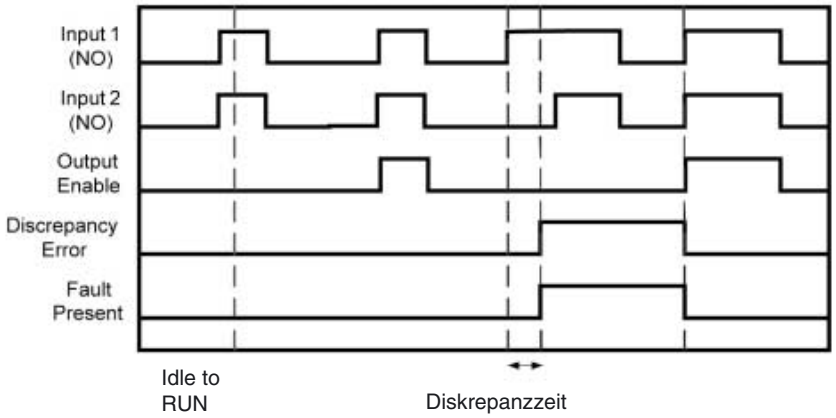
Maximale Anzahl von Ausgängen für den Funktionsblock „Zustimmschalterüberwachung“

Fehlerbehandlung und Zurücksetzen des Fehlerzustands

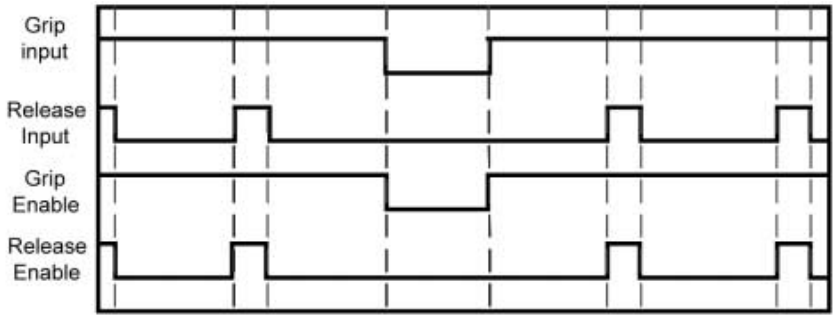
Fehlerzustand	Verhalten bei Fehlererkennung			Zurücksetzen des Fehlerzustands
	Output Enable	Fault Present	Fehlerausgang	
Discrepancy Error	AUS (Sicherheitszustand)	EIN	Discrepancy Error: EIN	Beheben Sie die Ursache des Fehlers, und entscheiden Sie sich dann für eine der folgenden Möglichkeiten: 1. Setzen Sie den Eingang auf AUS und dann wieder auf EIN, oder 2. ändern Sie den Betriebsmodus des Sicherheitsnetzwerk-Controllers NE1A nach IDLE und dann wieder nach RUN.

Signalverhalten

Normaler Betrieb und Diskrepanzfehler:

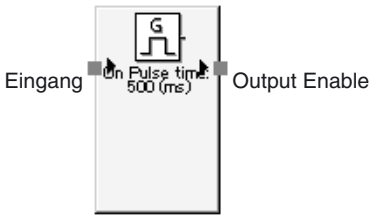


Greifsignal und Freigabesignal:



6-5-14 Funktionsblock: Impulsgeber

Diagramm



Standardbelegung (Ein- und Ausgänge)

Allgemeine Beschreibung

Diese Funktion steht nur beim Sicherheitsnetzwerk-Controller NE1A ab Geräteversion 1.0 zur Verfügung.

Der Funktionsblock „Pulse Generator“ erzeugt einen EIN/AUS-Impuls am Signal „Output Enable“, während das Eingangssignal des Funktionsblocks EIN ist.
Ein- und Ausschaltdauer des Impulses können unabhängig voneinander in 10-ms-Schritten zwischen 10 ms und 3 s eingestellt werden. Bei einer Einschaltdauer von 100 ms und einer Ausschaltdauer von 500 ms wird das Signal immer wieder für 100 ms aktiviert (EIN) und dann für 500 ms deaktiviert (AUS).

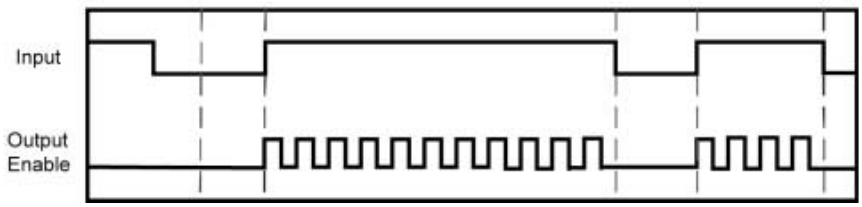
Hinweis Die Fehlertoleranz der Ausgangsimpulslänge entspricht der Zykluszeit. Wenn beispielsweise bei einer Zykluszeit von 7 ms eine Impulsdauer von 100 ms eingestellt ist, beträgt der Ausgangsimpuls 93 bis 107 ms.

Parametereinstellungen

Einstellung	Einstellbereich	Standardeinstellung
ON Pulse Time	10 ms bis 3 s (in 10-ms-Schritten)	500 ms
OFF Pulse Time	10 ms bis 3 s (in 10-ms-Schritten)	500 ms

Der Zeitsollwert muss größer sein die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A.

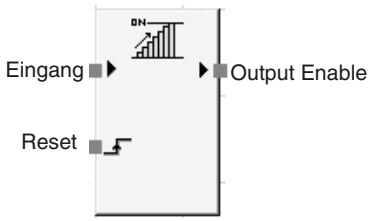
Zeitablaufdiagramm



IDLE RUN

6-5-15 Funktionsblock: Zähler

Diagramm



Standardbelegung (Ein- und Ausgänge)

Allgemeine Beschreibung

Diese Funktion steht nur beim Sicherheitsnetzwerk-Controller NE1A ab Geräteversion 1.0 zur Verfügung.

Der Funktionsblock „Counter“ zählt die Eingangsimpulse an einem Eingang und setzt das Signal „Output Enable“ auf EIN, wenn der Zählerwert einen Sollwert (SV) erreicht, der zuvor mit dem „Netzwerkkonfigurator“ eingestellt wurde. Die Funktion zählt, wie oft das Eingangssignal von AUS nach EIN wechselt.

Wenn die Eingangszählung den voreingestellten Sollwert erreicht, wird das Signal „Output Enable“ auf EIN gesetzt und dort gehalten. Damit die Impulse des Eingangssignals erkannt werden können, müssen Ein- und Ausschaltzeit des Eingangsimpulses länger sein als die Zykluszeit.

■ Rücksetzmethoden (Rücksetzbedingung)

Die Rücksetzbedingung zum Zurücksetzen des Eingangszählers (Istwert) kann als „Manual Reset“ oder als „Auto Reset“ konfiguriert werden.

Wenn die Rücksetzbedingung als „Auto Reset“ konfiguriert wurde und der Eingangszähler den in den Konfigurationsdaten eingestellten Sollwert erreicht, wird das Signal „Output Enable“ auf EIN gesetzt und solange gehalten, wie das Eingangssignal aktiviert ist (EIN). Wenn das Eingangsignal nach AUS wechselt, wird der Eingangszähler zurückgesetzt.

Wenn die Rücksetzbedingung als „Manual Reset“ konfiguriert wurde, wird der Eingangszähler zurückgesetzt und das Signal „Output Enable“ auf AUS gesetzt, sobald das Signal „Reset“ nach EIN wechselt. Es werden keine Eingangsimpulse gezählt, solange das Signal „Reset“ aktiviert ist (EIN).

■ Zählmethoden (Count Type)

„Count Type“ kann als „Down counter“ oder als „Up counter“ (Ab- oder Aufwärtszähler) konfiguriert werden.

Bei einem Abwärtszähler entspricht der voreingestellte Sollwert dem Ausgangswert des Zählers, und der Zähler vermindert den Zählerwert jedes Mal um den Betrag 1, wenn ein Eingangsimpuls erkannt wird. Das Signal „Output Enable“ wird aktiviert (EIN), sobald der Zählerwert 0 erreicht ist.

Der Zählersollwert dieses Funktionsblocks wird im internen Arbeitsbereich des Funktionsblocks gespeichert und kann mit einem Programmiergerät überwacht werden.

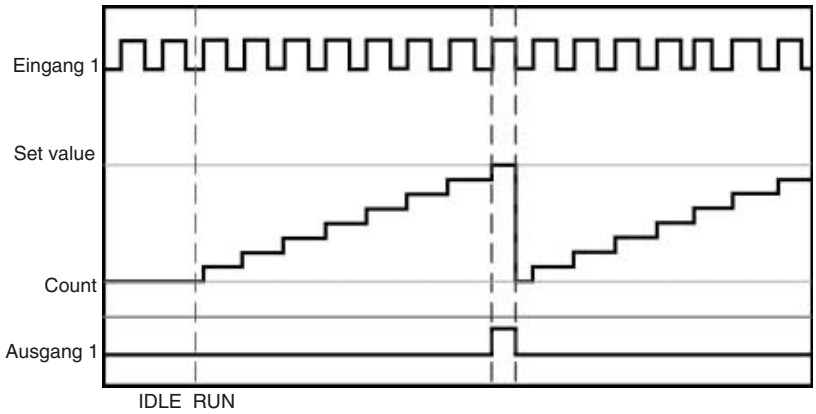
Bei einem Aufwärtszähler lautet der Ausgangswert des Zählers 0, und der Zähler erhöht den Zählerwert jedes Mal um den Betrag 1, wenn ein Eingangsimpuls erkannt wird. Das Signal „Output Enable“ wird aktiviert (EIN), sobald der Zählerwert den voreingestellten Sollwert erreicht.

Parametereinstellungen

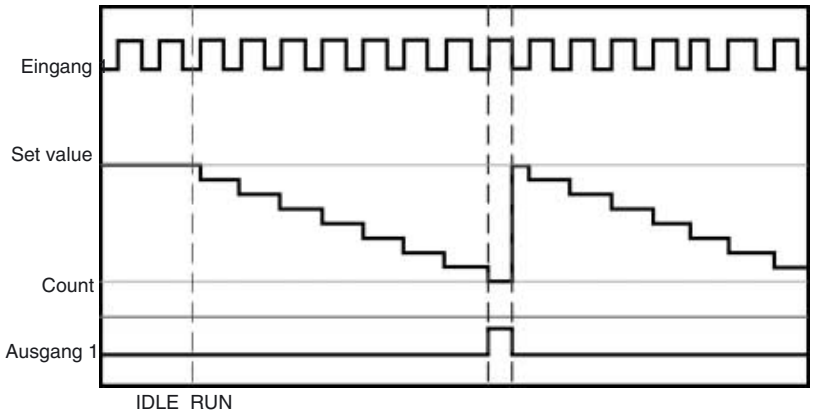
Einstellung	Einstellbereich	Standardeinstellung
Reset Condition	Auto Reset Manual Reset	Manual Reset
Count Type	Down counter (Abwärtszähler) Up counter (Aufwärtszähler)	Down counter (Abwärtszähler)
Counter	1 bis 65.535 (Zählerwert)	1 (Zählerwert)

Signalverhalten

1. Automatische Rücksetzung
   Aufwärtszähler:

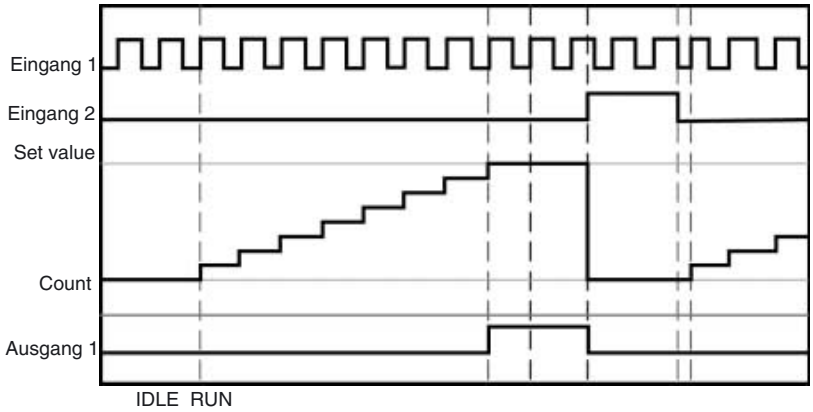


Abwärtszähler:

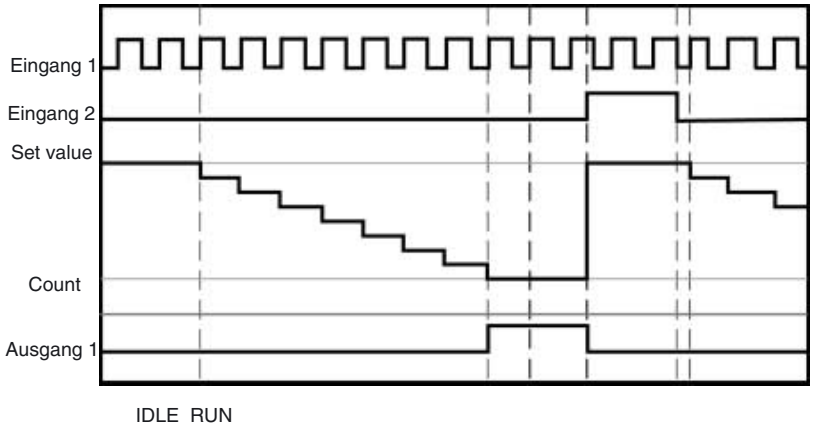


2. Manuelle Rücksetzung

Abwärtszähler:

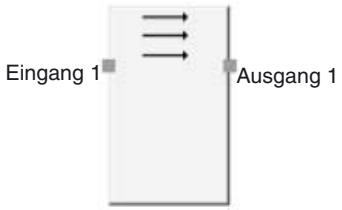


Abwärtszähler:



6-5-16 Logikfunktion: Multi Connector

Diagramm



Standardbelegung (Ein- und Ausgänge)

Allgemeine Beschreibung

Diese Funktion steht nur beim Sicherheitsnetzwerk-Controller NE1A ab Geräteversion 1.0 zur Verfügung.

Die Funktion „Multi Connector“ übermittelt Eingangssignale (bis zu 8 Eingänge) an Ausgangssignale (bis zu 8 Ausgänge).
Die Ein- und Ausgangssignale werden einander einzeln von 1 bis 8 zugewiesen. Der Status anderer Eingangssignale spielt keine Rolle.

Optionale Ausgangseinstellungen

Die Anzahl der Ausgänge kann auf der Registerkarte „In/Out Setting“ des Eigenschaftendialogfelds der Logikfunktion auf einen Wert zwischen 1 und 8 eingestellt werden.

Einstellung	Einstellbereich	Standardeinstellung
Number of Inputs	1 bis 8	1

Logikfunktion „Multi Connector“ mit der maximal möglichen Zahl von Ausgängen

Wahrheitstabellen

■ **Multi-Connector-Wahrheitstabelle:**

Eingang								Ausgänge							
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
0	x	x	x	x	x	x	x	0	x	x	x	x	x	x	x
1	x	x	x	x	x	x	x	1	x	x	x	x	x	x	x
x	0	x	x	x	x	x	x	x	0	x	x	x	x	x	x
x	1	x	x	x	x	x	x	x	1	x	x	x	x	x	x
x	x	0	x	x	x	x	x	x	x	0	x	x	x	x	x
x	x	1	x	x	x	x	x	x	x	1	x	x	x	x	x
x	x	x	0	x	x	x	x	x	x	x	0	x	x	x	x
x	x	x	1	x	x	x	x	x	x	x	1	x	x	x	x
x	x	x	x	0	x	x	x	x	x	x	x	0	x	x	x
x	x	x	x	1	x	x	x	x	x	x	x	1	x	x	x
x	x	x	x	x	0	x	x	x	x	x	x	x	0	x	x
x	x	x	x	x	1	x	x	x	x	x	x	x	1	x	x
x	x	x	x	x	x	0	x	x	x	x	x	x	x	0	x
x	x	x	x	x	x	1	x	x	x	x	x	x	x	1	x
x	x	x	x	x	x	x	0	x	x	x	x	x	x	x	0
x	x	x	x	x	x	x	1	x	x	x	x	x	x	x	1

0: AUS, 1: EIN, x: wahlweise EIN oder AUS

ABSCHNITT 7
Sonstige Funktionen

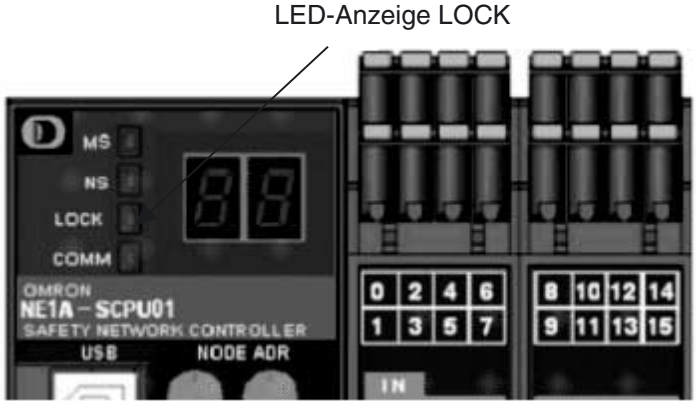
7-1 Konfigurationsschutz 178
7-2 Rücksetzung 179
7-2-1 Rücksetzvarianten 179
7-2-2 Rücksetzvarianten und Zustand des Sicherheitsnetzwerk-Controllers NE1A 179
7-3 Zugangsbeschränkung durch Kennwort 180
7-3-1 Der Zugangsbeschränkung unterliegende Operationen 180
7-3-2 Verlorengegangenes Kennwort 180

7-1 Konfigurationsschutz

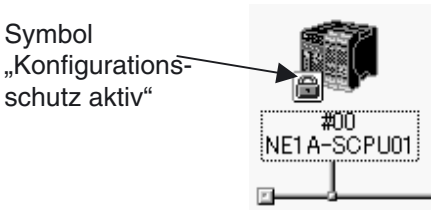
Die im Sicherheitsnetzwerk-Controller NE1A gespeicherten heruntergeladenen und verifizierten Konfigurationsdaten können mithilfe des Netzwerkkonfigurators geschützt werden. Wurden die Konfigurationsdaten geschützt, können sie nur nach Aufheben des Schutzes geändert werden.

Beim Schutz der Konfigurationsdaten werden die folgenden Anzeigen usw. gesetzt.

- Die LED-Anzeige „LOCK“ an der Front des Sicherheitsnetzwerk-Controllers NE1A leuchtet gelb. (Sind die Konfigurationsdaten nicht geschützt, blinkt diese LED-Anzeige gelb.)



- Im Netzwerkkonfigurator wird das Symbol „Konfigurationsschutz aktiv“ angezeigt.



7-2 Rücksetzung

7-2-1 Rücksetzvarianten

Der Netzwerkkonfigurator kann den Sicherheitsnetzwerk-Controller NE1A auf dreierlei Weise zurücksetzen. Das Zurücksetzen erfordert die Eingabe eines Kennworts.

Rücksetzvariante	Konfigurationsdaten	Fehlerprotokoll
Emulate cycling power	Die Einstellungen vor dem Zurücksetzen bleiben erhalten.	Der Protokollzustand vor dem Zurücksetzen bleibt erhalten.
Return to the default configuration, and then emulate cycling power (Initialisierung aller Daten)	Initialisierung auf Standardeinstellung	Initialisierung (Alle Daten werden gelöscht)
Return to the default configuration except to preserve the following parameters, and then emulate cycling power (Erhaltung bestimmter Daten)	Abhängig von Anwendereinstellungen	Initialisierung (Alle Daten werden gelöscht)

Zu den Konfigurationsdaten gehören die Einstellungen für die DeviceNet-Kommunikation (DeviceNet Safety und DeviceNet), Geräteparameter wie E/A-Einstellungen, Anwenderprogramm und Kennwörter.

Der Sicherheitsnetzwerk-Controller speichert diese Daten in seinem nichtflüchtigen Speicher. Bestimmte Informationen können nach dem Setzen nicht mehr geändert werden. Wählen Sie bei Bedarf die entsprechende Rücksetzvariante aus, um diese Informationen wieder auf die Standardeinstellungen zurückzusetzen.

Wartungsdaten wie zum Beispiel Gesamteinschaltdauer, Schaltspielzähler-Überwachungseinstellungen oder Überwachungswerte für lokale E/A-Punkte und Testausgänge werden jedoch je nach verwendeter Rücksetzvariante nicht gelöscht.

Informationen zu den konfigurierbaren Parametern finden Sie im *DeviceNet-Sicherheitssystem-Konfigurationshandbuch (Cat. No. Z905)*.

7-2-2 Rücksetzvarianten und Zustand des Sicherheitsnetzwerk-Controllers NE1A

Je nach Zustand des Sicherheitsnetzwerk-Controllers NE1A können bestimmte Rücksetzvarianten nicht eingesetzt werden.

Rücksetzvariante	Zustand des Sicherheitsnetzwerk-Controllers NE1A			
	RUN / Konfiguration geschützt - LED-Anzeige „MS“ leuchtet grün - LED-Anzeige „LOCK“ leuchtet	**RUN / Konfiguration ungeschützt - LED-Anzeige „MS“ leuchtet grün - LED-Anzeige „LOCK“ blinkt**	**Anderer Betriebsmodus (nicht RUN) / Konfiguration geschützt - LED-Anzeige „MS“ leuchtet nicht grün - LED-Anzeige „LOCK“ leuchtet**	**Anderer Betriebsmodus (nicht RUN) / Konfiguration ungeschützt - LED-Anzeige „MS“ leuchtet nicht grün - LED-Anzeige „LOCK“ blinkt oder aus**
Emulate cycling power	Möglich	Möglich	Möglich	Möglich
Return to the default configuration, and then emulate cycling power	Nicht möglich	Möglich	Nicht möglich	Möglich
Return to the default configuration except to preserve the following parameters, and then emulate cycling power.	Nicht möglich	Möglich	Nicht möglich	Möglich

Hinweis Nach Herstellung einer Sicherheits-E/A-Verbindung ist ein Rücksetzen nicht möglich.

7-3 Zugangsbeschränkung durch Kennwort

Der Sicherheitsnetzwerk-Controller NE1A kann in seinem nichtflüchtigem Speicher ein Kennwort speichern, um den unerwarteten oder unautorisierten Zugriff auf den Sicherheitsnetzwerk-Controller NE1A durch unbefugte Personen zu verhindern. Standardmäßig ist kein Kennwort eingestellt. Soll eine Zugangsbeschränkung realisiert werden, muss explizit ein Kennwort eingestellt werden.

Verwenden Sie zum Einrichten und Ändern des Kennworts für den Sicherheitsnetzwerk-Controller NE1A den Netzwerkkonfigurator. Informationen bezüglich der Vorgehensweise beim Einrichten des Kennworts mit dem Netzwerkkonfigurator finden Sie unter *3-6 Kennwortschutz für Geräte* im *DeviceNet Safety System Konfigurationshandbuch* (Cat. No. Z905).

7-3-1 Der Zugangsbeschränkung unterliegende Operationen

Die folgenden Operationen erfordern die Eingabe des Kennworts (sofern gesetzt):

- Herunterladen von Konfigurationsdaten
- Setzen und Aufheben des Konfigurationsschutzes
- Zurücksetzen des Sicherheitsnetzwerk-Controllers NE1A
- Wechsel des Betriebsmodus
- Ändern des Kennworts

7-3-2 Verlorengegangenes Kennwort

Sollte das Kennwort verloren gegangen sein, so wenden Sie sich an den OMRON Vertrieb.

ABSCHNITT 8
Betriebsmodi und Verhalten bei Spannungseinbrüchen und -ausfällen

8-1 Betriebsmodi des Sicherheitsnetzwerk-Controllers NE1A 182
8-1-1 Übersicht über die Betriebsmodi 182
8-1-2 Bestimmung des Betriebsmodus 183
8-1-3 In den einzelnen Betriebsmodi unterstützte Funktionen 184
8-1-4 Parameter „Operating Mode at Startup“ 185
8-1-5 Änderungen des Betriebsmodus 185
8-2 Verhalten bei Spannungseinbrüchen und -ausfällen 186
8-2-1 Verhalten bei Spannungseinbrüchen 186
8-2-2 Automatisches Wiederaufsetzen nach Spannungseinbrüchen 186

8-1 Betriebsmodi des Sicherheitsnetzwerk-Controllers NE1A

8-1-1 Übersicht über die Betriebsmodi

Der Sicherheitsnetzwerk-Controller NE1A verfügt über die folgenden Betriebsmodi:

SELF-DIAGNOSTIC (Selbstdiagnose)

Der Sicherheitsnetzwerk-Controller NE1A führt eine interne Selbstdiagnose zur Sicherstellung der ordnungsgemäßen Funktion der Sicherheitsfunktionen durch.

CONFIGURING (Konfigurieren)

Der Sicherheitsnetzwerk-Controller NE1A-SCPU01 wartet auf den Abschluss der Konfiguration durch den Netzwerkkonfigurator. Der Sicherheitsnetzwerk-Controller NE1A wechselt in diesen Modus, wenn er nach Abschluss der Initialisierung noch nicht konfiguriert ist oder ein Fehler in den Konfigurationsdaten vorliegt.

IDLE (Leerlauf)

Der Sicherheitsnetzwerk-Controller NE1A-SCPU01 wartet nach Abschluss der Initialisierung auf den Wechsel in den Betriebsmodus RUN.

Nicht sicherheitsrelevante Steuerungskomponenten (Standard-E/A-Kommunikation, Message-Kommunikation usw.) sind in Funktion.

RUN (Betrieb)

Sicherheitsrelevante (Anwenderprogramm, Sicherheits-E/A-Kommunikation, Aktualisierungssteuerung der Sicherheits-E/A) und nicht sicherheitsrelevante Steuerungskomponenten (Standard-E/A-Kommunikation, Message-Kommunikation usw.) sind in Funktion.

ABORT (Abbruch-Zustand)

Der Sicherheitsnetzwerk-Controller NE1A wechselt in den Abbruch-Zustand, wenn nach Abschluss der Konfiguration eine Schaltereinstellung geändert wird. In diesem Fall hält der Sicherheitsnetzwerk-Controller NE1A alle Funktionen mit Ausnahme der Message-Kommunikation an und versetzt sie in den Sicherheitszustand.

Erfordert eine Änderung der Systemkonfiguration die Änderung der Schaltereinstellungen des Sicherheitsnetzwerk-Controllers NE1A, muss dieser anschließend zurückgesetzt werden. Details zur Rücksetzfunktion finden Sie in *Kapitel 7: Sonstige Funktionen*.

CRITICAL ERROR (Kritischer-Fehler-Zustand)

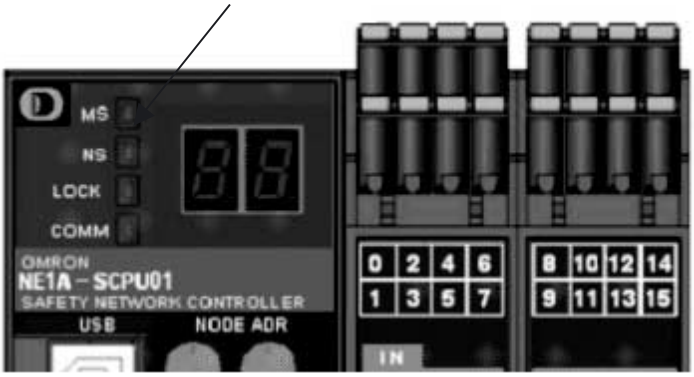
Beim Auftreten eines kritischen Fehlers wechselt der Sicherheitsnetzwerk-Controller NE1A in diesen Betriebsmodus.
In diesem Fall hält der Sicherheitsnetzwerk-Controller NE1A alle Funktionen an und versetzt sie in den Sicherheitszustand.

8-1-2 Bestimmung des Betriebsmodus

Bestimmung mithilfe der LED-Anzeige „MS“

Die LED-Anzeige „MS“ an der Front des Sicherheitsnetzwerk-Controllers NE1A ermöglicht die Bestimmung des aktuellen Betriebsmodus.

LED-Anzeige „MS“ (Baugruppenstatus)



Bezeichnung der LED-Anzeige	Farbe	Status	Bedeutung
MS (Baugruppen-status)	Grün	Leuchtet	RUN (Betrieb)
		Blinkt	IDLE (Leerlauf)
	Rot	Leuchtet	Kritischer Fehler
		Blinkt	Abbruch
	Grün/Rot	Blinkt	Selbstdiagnose, Warten auf TUNID-Einstellung oder Warten auf Konfiguration
	-	AUS	Spannungsversorgung ausgeschaltet

: Leuchtet : Blinkt : AUS

Betriebsmodus-Überprüfung mithilfe des Betriebsmodus-Merkers

Bit 6 (Betriebsmodus-Merker) des allgemeinen Baugruppenstatus gibt an, ob sich der Sicherheitsnetzwerk-Controller NE1A im RUN-Modus befindet oder nicht.

8-1-3 In den einzelnen Betriebsmodi unterstützte Funktionen

Die nachstehende Tabelle gibt die in den verschiedenen Betriebsmodi des Sicherheitsnetzwerk-Controllers NE1A vorliegenden Zustände verschiedener Funktionsmerkmale und die in diesen Betriebsmodi unterstützten Operationen des Netzwerkkonfigurators an.

Betriebsmodus	Sicherheitsfunktionen			Standardfunktionen		Operationen des Netzwerkkonfigurators z (siehe Hinweis 1)				
	Anwenderprogramm	Sicherheits-E/A-Kommunikation	Steuerung lokaler E/A-Punkte (einschl. Testausgänge)	Standard-E/A-Kommunikation	Message-Kommunikation	Konfiguration	Konfigurationsschutz setzen/aufheben	Rücksetzung	Kennwortänderung	Online-Überwachung
RUN	Unterstützt	Unterstützt	Aktualisiert	Unterstützt	Unterstützt	Unterstützt (siehe Hinweis 3)	Unterstützt	Unterstützt (siehe Hinweis 4)	Unterstützt	Unterstützt
IDLE	Angehalten	Angehalten	Sicherheitszustand	Unterstützt (Siehe Hinweis 2)	Unterstützt	Unterstützt (siehe Hinweis 3)	Unterstützt	Unterstützt (siehe Hinweis 4)	Unterstützt	Unterstützt
CONFIGURING	Angehalten	Angehalten	Sicherheitszustand	Angehalten	Unterstützt	Unterstützt	Nicht unterstützt	Unterstützt	Unterstützt	Unterstützt
ABORT	Angehalten	Angehalten	Sicherheitszustand	Angehalten	Unterstützt	Nicht unterstützt	Nicht unterstützt	Unterstützt (siehe Hinweis 4)	Unterstützt	Unterstützt
CRITICAL ERROR	Angehalten	Angehalten	Sicherheitszustand	Angehalten	Angehalten	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
INITIALIZATION	Angehalten	Angehalten	Sicherheitszustand	Angehalten	Angehalten	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

Hinweis

(1) Operationen des Netzwerkkonfigurators erfordern möglicherweise die Eingabe eines Kennworts.
Details hierzu finden Sie in Kapitel 7: Sonstige Funktionen.

(2) Bei einer Änderung des Betriebsmodus des Sicherheitsnetzwerk-Controllers NE1A von „RUN“ nach „IDLE“ hängen die Eingangsdaten des Masters von der Halteeinstellung für den E/A-Bereich von Standard-Slaves ab. Details hierzu finden Sie in Kapitel 4: DeviceNet-Kommunikationsfunktionen.

(3) Je nach Einstellung des Konfigurationsschutzes. Details hierzu finden Sie in Kapitel 7: Sonstige Funktionen.

(4) Je nach Rücksetzvariante und Einstellung des Konfigurationsschutzes. Details hierzu finden Sie in Kapitel 7: Sonstige Funktionen.

8-1-4 Parameter „Operating Mode at Startup“

Mithilfe des Parameters „Operating Mode at Startup“ können Sie festlegen, in welchen Betriebsmodus der Sicherheitsnetzwerk-Controller NE1A beim Einschalten der Versorgungsspannung nach erfolgreich durchgeführter Konfiguration wechselt. Für diesen Parameter bestehen die beiden in der nachstehenden Tabelle aufgeführten Auswahlmöglichkeiten.

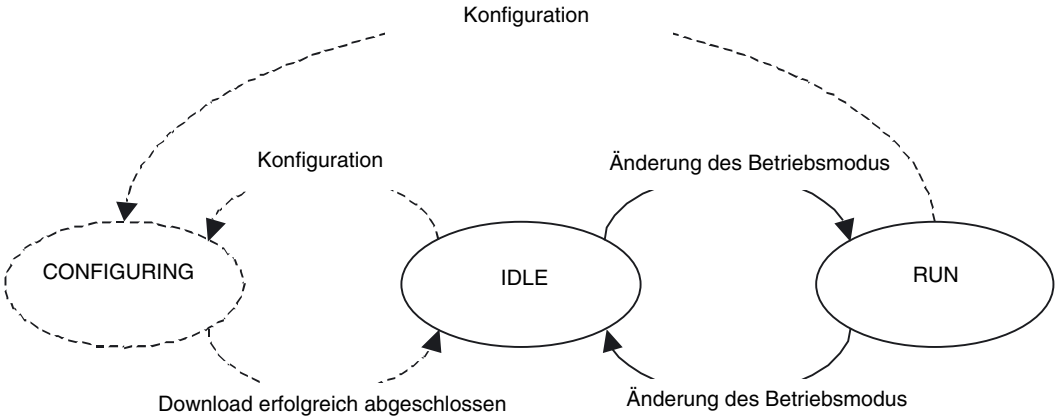
Operating mode on startup	Beschreibung
Normal Mode	Der Sicherheitsnetzwerk-Controller NE1A wechselt nach Abschluss der Konfiguration in den Betriebsmodus „IDLE“. Die Umschaltung in den Betriebsmodus „RUN“ muss bei jedem Start durch explizite Änderung des Betriebsmodus mithilfe des Netzwerkkonfigurators erfolgen.
Automatic Execution Mode	Bei Auswahl dieser Einstellung wechselt der Sicherheitsnetzwerk-Controller NE1A nach den folgenden Ereignissen automatisch in den Betriebsmodus „RUN“. • Konfigurationsschutz • Unterbrechungen der Versorgungsspannung, nachdem der Sicherheitsnetzwerk-Controller NE1A-SCPU01 einmal in den Betriebsmodus „RUN“ versetzt wurde.

WICHTIG Selbst wenn für den Parameter „Operating Mode at Startup“ die Einstellung „Automatic Execution Mode“ gewählt und die Konfiguration geschützt wurde, startet der Sicherheitsnetzwerk-Controller NE1A beim Einschalten der Versorgungsspannung nicht im Betriebsmodus „RUN“, wenn er sich beim vorherigen Ausschalten der Versorgungsspannung im Betriebsmodus „IDLE“ befand. Damit der Sicherheitsnetzwerk-Controller NE1A-SCPU01 im Betriebsmodus „RUN“ startet, muss er sich vor dem Ausschalten der Versorgungsspannung auch in diesem Betriebsmodus befunden haben.

8-1-5 Änderungen des Betriebsmodus

Der Betriebsmodus des Sicherheitsnetzwerk-Controllers NE1A kann mithilfe des Netzwerkkonfigurators geändert werden.
Hierfür ist möglicherweise die Eingabe eines Kennworts erforderlich.

- IDLE → RUN
- RUN → IDLE



8-2 Verhalten bei Spannungseinbrüchen und -ausfällen

8-2-1 Verhalten bei Spannungseinbrüchen

Spannungseinbruch bei der Versorgungsspannung der internen Schaltkreise

Fällt die Versorgungsspannung der internen Schaltkreise auf unter 85 % der Nennspannung ab, schaltet der Sicherheitsnetzwerk-Controller NE1A die Ausgänge aus.

Spannungseinbruch bei der Versorgungsspannung der E/A-Schaltkreise

Fällt die Versorgungsspannung der Eingänge auf unter 85 % der Nennspannung ab, während die Versorgungsspannung der internen Schaltkreise auf normalem Niveau bleibt, setzt der Sicherheitsnetzwerk-Controller NE1A den Betrieb fort, ohne jedoch die Eingänge weiterhin zu aktualisieren. Analog gilt: Fällt die Versorgungsspannung der Ausgänge auf unter 85 % der Nennspannung ab, während die Versorgungsspannung der internen Schaltkreise auf normalem Niveau bleibt, setzt der Sicherheitsnetzwerk-Controller den Betrieb fort, ohne jedoch die Ausgänge weiterhin zu aktualisieren.

Die Überwachungsfunktion des Sicherheitsnetzwerk-Controllers NE1A für die E/A-Versorgungsspannung ermöglicht die Überwachung der E/A-Versorgungsspannung.

8-2-2 Automatisches Wiederaufsetzen nach Spannungseinbrüchen

Wiederaufsetzen nach einem Spannungseinbruch bei der Versorgungsspannung der internen Schaltkreise

Hat sich die Versorgungsspannung nach einem durch eine Schwankung der Versorgungsspannung bedingten Einbruch wieder erholt (auf mindestens 85 % der Nennspannung), kann einer der beiden folgenden Fälle eintreten:

1. Der Betrieb wieder automatisch wieder aufgenommen
2. Es tritt ein kritischer Fehler auf, zur Wiederaufnahme des Betriebs muss die Versorgungsspannung des Sicherheitsnetzwerk-Controller NE1A-SCPU01 aus- und wieder eingeschaltet werden

Ursächlich hierfür ist, dass der Betrieb des Sicherheitsnetzwerk-Controllers NE1A instabil wird und dieser einen Selbstdiagnosefehler erkennt. Der erstgenannte Fall (1) tritt ein, wenn die Versorgungsspannung des Sicherheitsnetzwerk-Controllers NE1A vollständig ausgefallen ist, der letztgenannte Fall (2) tritt ein, wenn die Versorgungsspannung um den unteren Grenzwert der internen Spannungseinbrucherkennungsschaltung schwankt.

Wiederaufsetzen nach einem Spannungseinbruch bei der Versorgungsspannung der E/A-Schaltkreise

Die E/A-Aktualisierung wird automatisch wieder aufgenommen, sobald sich die Versorgungsspannung für die E/A-Schaltkreise erholt hat (auf mindestens 85 % der Nennspannung). Der E/A-Spannungsversorgungsüberwachungsfehler wird ebenfalls automatisch gelöscht.

ABSCHNITT 9
Kommunikationsvermögen der dezentralen E/A und Ansprechzeit der lokalen E/A

9-1 Übersicht 188
9-2 Betriebsablauf und Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A 189
9-3 E/A-Aktualisierungszykluszeit und Netzwerkreaktionszeit 191
9-4 Reaktionszeit 193
9-4-1 Reaktionszeitkonzepte 193
9-4-2 Berechnung der Reaktionszeit 193
9-4-3 Überprüfung der Reaktionszeit 198

9-1 Übersicht

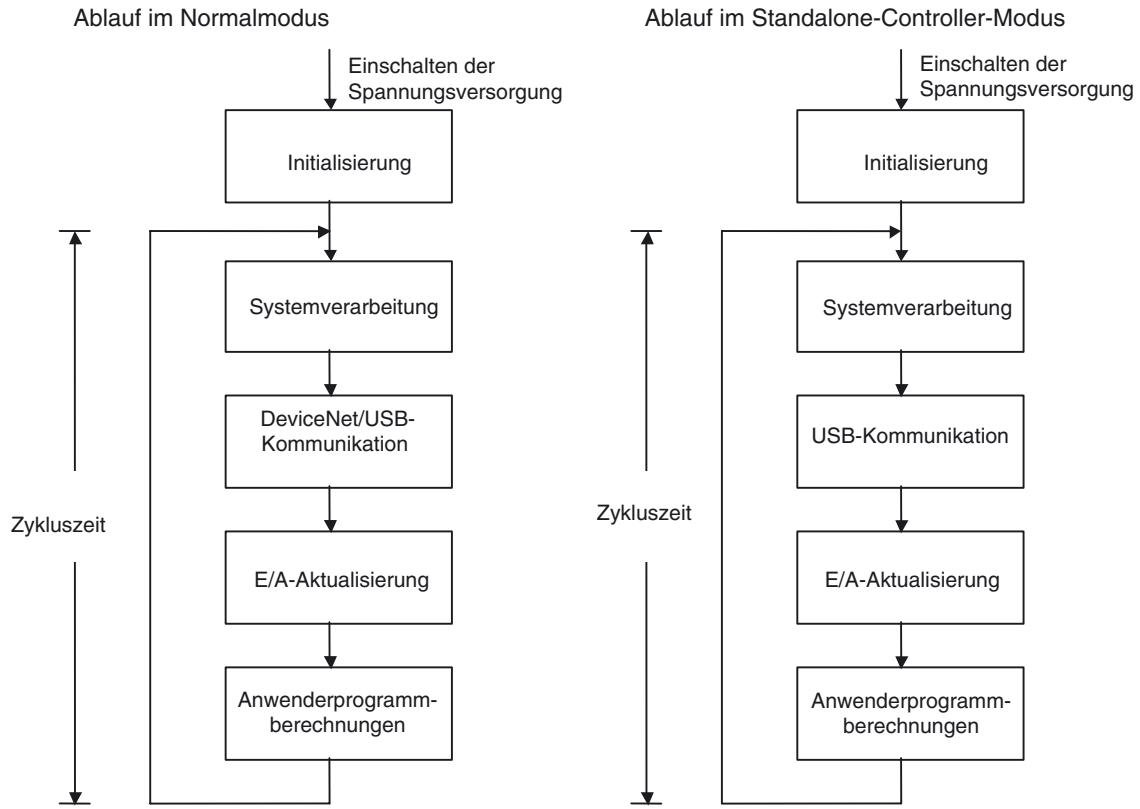
Dieses Kapitel befasst sich mit dem Kommunikationsvermögen der dezentralen E/A und der Ansprechzeit der lokalen E/A.
Die hier durchgeführten Berechnungen setzen voraus, dass die folgenden Bedingungen erfüllt sind:

- Die Konfiguration ist gültig.
- Die Versorgungsspannung wurde eingeschaltet, die Selbstdiagnose wurde erfolgreich abgeschlossen und der Sicherheitsnetzwerk-Controller NE1A befindet sich im Betriebsmodus „RUN“.
- Die benötigten Sicherheits-Slaves wurden in das System eingebunden.

9-2 Betriebsablauf und Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A

Dieser Abschnitt skizziert den Ablauf der Operationen des Sicherheitsnetzwerk-Controllers NE1A.

Beim Einschalten der Versorgungsspannung führt der Sicherheitsnetzwerk-Controller NE1A eine interne Initialisierung durch. Sofern keine Fehler auftreten, durchläuft der Sicherheitsnetzwerk-Controller NE1A anschließend einen zyklischen Ablauf aus Systemverarbeitung, DeviceNet/USB-Kommunikation, E/A-Aktualisierung und Ausführung des Anwenderprogramms.
Im Standalone-Controller-Modus entfallen in diesem Zyklus die DeviceNet-Prozesse. Die Zykluszeit hängt vom Umfang des Anwenderprogramms und der Konfiguration der DeviceNet-Kommunikation mit den dezentralen E/A-Baugruppen ab.



Hinweis Die Initialisierung nach dem Einschalten der Versorgungsspannung nimmt ca. 6 s in Anspruch. Im Rahmen der Initialisierung erfolgt die für die Sicherstellung der ordnungsgemäßen Funktion der Sicherheitsfunktionen des Sicherheitsnetzwerk-Controllers NE1A erforderliche Selbstdiagnose.

Die Zykluszeit berechnet sich nach der folgenden Formel:

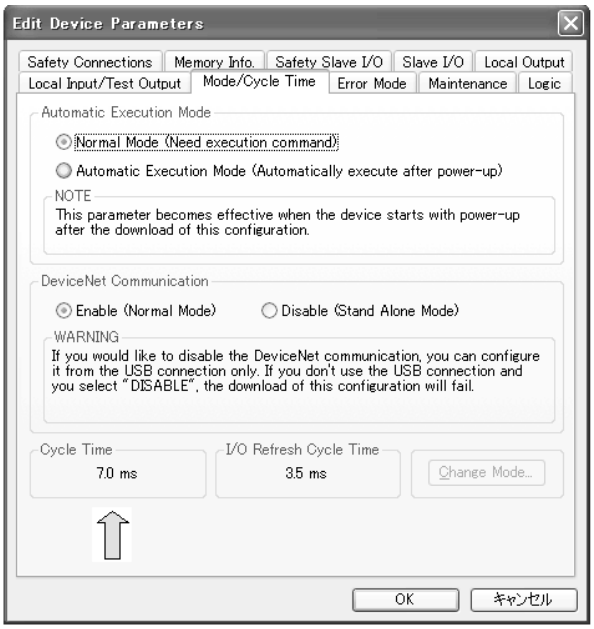
Controller-Zykluszeit = Systemverarbeitungszeit
+ Kommunikationszeit (DeviceNet und/oder USB)
+ E/A-Aktualisierungszeit
+ Ausführungszeit für das Anwenderprogramm

Je nach Konfiguration kann die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A mit einer Auflösung von einer Millisekunde eingestellt werden. Die Zykluszeit kann mithilfe des Netzwerkkonfigurators überprüft werden.

Hinweis Nach dem Start des Sicherheitsnetzwerk-Controllers NE1A wird die DeviceNet-Verbindung hergestellt. Danach werden die Geräte überprüft, damit die DeviceNet Sicherheits-E/A-Kommunikation beginnen kann. Dieser Vorgang kann je nach Konfiguration (z.B. eingestellte Anzahl von Verbindungen) bis zu 2 s in Anspruch nehmen. Die folgende Formel berechnet die Zeitspanne zwischen dem Herstellen der obigen Verbindung bis zum Senden und Empfangen von E/A-Daten über diese Verbindung.
(Verarbeitungszeit nach dem Verbindungsaufbau bis zum Senden und Empfangen von E/A-Daten) =
EPI-Einstellung x 3 + Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A x 6

Hinweis Nach seiner Initialisierung wird der Sicherheitsnetzwerk-Controller NE1A dem DeviceNet-Netzwerk hinzugefügt, sobald bestätigt wurde, dass keine Adressdoppelungen im DeviceNet-Netzwerk vorkommen. Dieser Vorgang nimmt ungefähr 2 s in Anspruch und wird nicht vor Beginn des Betriebs abgeschlossen, wenn der Sicherheitsnetzwerk-Controller für die automatische Ausführung beim Einschalten der Spannungsversorgung konfiguriert wurde. Auch diese Zeit muss berücksichtigt werden, wenn es um die Zeitspanne bis zum Erhalt gültiger DeviceNet-Daten per E/A-Kommunikation geht.

Die E/A-Aktualisierungszykluszeit des Sicherheitsnetzwerk-Controllers NE1A kann auf der Registerkarte „Mode/Cycle Time“ des Dialogfelds „Edit Device Parameters“ überprüft werden.


Edit Device Parameters
Safety Connections
Memory Info.
Safety Slave I/O
Slave I/O
Local Output
Local Input/Test Output
Mode/Cycle Time
Error Mode
Maintenance
Logic
Automatic Execution Mode
Normal Mode (Need execution command)
Automatic Execution Mode (Automatically execute after power-up)
NOTE
This parameter becomes effective when the device starts with power-up after the download of this configuration.
DeviceNet Communication
Enable (Normal Mode)
Disable (Stand Alone Mode)
WARNING
If you would like to disable the DeviceNet communication, you can configure it from the USB connection only. If you don't use the USB connection and you select "DISABLE", the download of this configuration will fail.
Cycle Time
7.0 ms
I/O Refresh Cycle Time
3.5 ms
Change Mode...
OK
キャンセル

Hinweis Das für EPI eingestellte Minimum entspricht entweder der Zykluszeit des Sicherheitsnetzwerk-Controllers oder der Zykluszeit der Sicherheits-Slaves (immer 6 ms) - je nach dem, welcher Wert größer ist. Folglich betrifft es den für EPI eingestellten Mindestwert, wenn die Zykluszeit des Sicherheitsnetzwerk-Controllers länger ist als 6 ms.

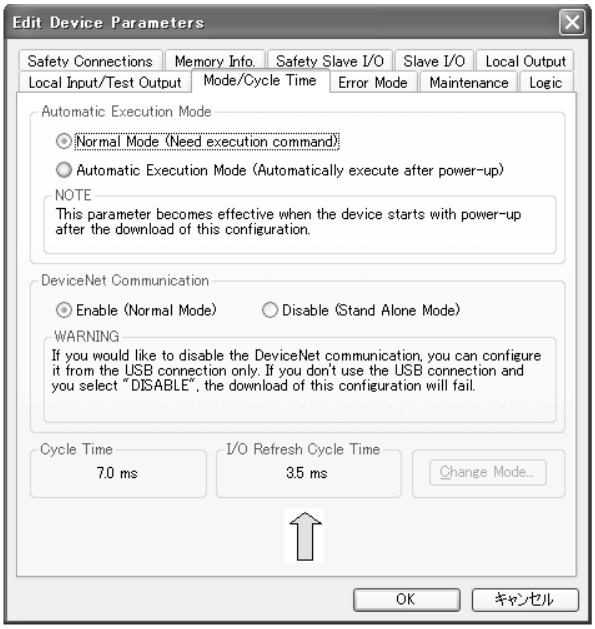
9-3 E/A-Aktualisierungszykluszeit und Netzwerkreaktionszeit

Anhand der E/A-Aktualisierungszykluszeit und der Netzwerkreaktionszeit können die lokale E/A-Reaktionszeit und das E/A-Kommunikationsvermögen des Sicherheitsnetzwerk-Controllers NE1A bestimmt werden.

E/A-Aktualisierungszeit

Zur Berechnung der lokalen E/A-Reaktionszeit wird die E/A-Reaktionszeit des Sicherheitsnetzwerk-Controllers NE1A herangezogen. Die E/A-Aktualisierungszykluszeit wird konfigurationsabhängig auf den optimalen Wert eingestellt. Folgende Werte stehen zur Auswahl: 3,5, 4,0, 4,5, 5,0, 5,5, 6,0 oder 6,5 ms. Die E/A-Aktualisierungszykluszeit kann mithilfe des Netzwerkkonfigurators überprüft werden.

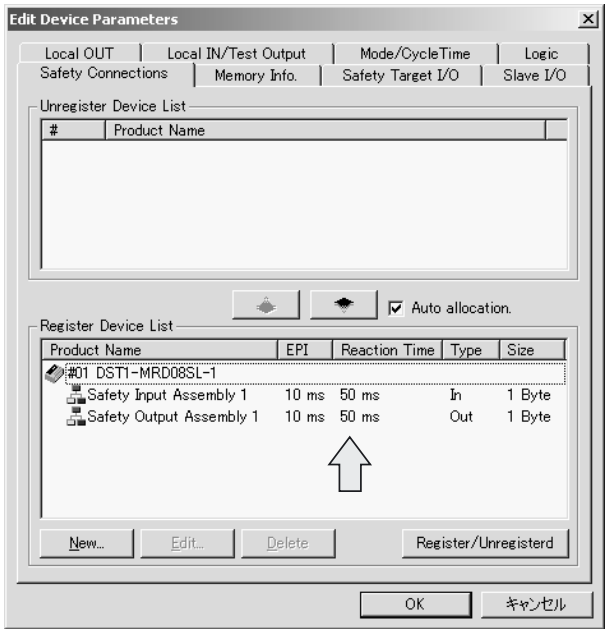
Die E/A-Aktualisierungszykluszeit des Sicherheitsnetzwerk-Controllers NE1A kann auf der Registerkarte „Mode/Cycle Time“ des Dialogfelds „Edit Device Parameters“ überprüft werden.


Edit Device Parameters
Safety Connections
Memory Info.
Safety Slave I/O
Slave I/O
Local Output
Local Input/Test Output
Mode/Cycle Time
Error Mode
Maintenance
Logic
Automatic Execution Mode
Normal Mode (Need execution command)
Automatic Execution Mode (Automatically execute after power-up)
NOTE
This parameter becomes effective when the device starts with power-up after the download of this configuration.
DeviceNet Communication
Enable (Normal Mode)
Disable (Stand Alone Mode)
WARNING
If you would like to disable the DeviceNet communication, you can configure it from the USB connection only. If you don't use the USB connection and you select "DISABLE", the download of this configuration will fail.
Cycle Time
7.0 ms
I/O Refresh Cycle Time
3.5 ms
Change Mode...
OK
キャンセル

Netzwerkreaktionszeit

Zur Berechnung der lokalen E/A-Reaktionszeit wird die E/A-Reaktionszeit des Sicherheitsnetzwerk-Controllers NE1A herangezogen.

Die Netzwerkreaktionszeit des Sicherheitsnetzwerk-Controllers kann auf der Registerkarte „Safety Connections“ des Dialogfelds „Edit Device Parameters“ überprüft werden.



9-4 Reaktionszeit

9-4-1 Reaktionszeitkonzepte

Die Reaktionszeit ist die unter Berücksichtigung von Fehlern und Ausfällen in der Sicherheitskette zum Anhalten des Maschinenbetriebs maximal erforderliche Zeit.
Die Reaktionszeit dient als Grundlage für die Berechnung des Sicherheitsabstands.

Die Reaktionszeit wird für jede Sicherheitskette einzeln berechnet. Nachstehend finden Sie einige Beispiele für typische Sicherheitsketten.

1. Lokale Eingabe / Lokale Ausgabe

2. Dezentrale Eingabe / Lokale Ausgabe

3. Lokale Eingabe / Dezentrale Ausgabe

4. Dezentrale Eingabe / Dezentrale Ausgabe

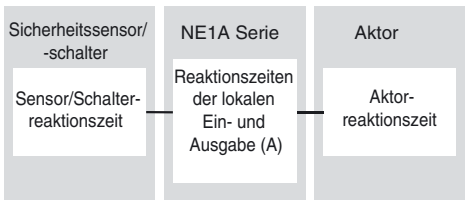
Hinweis Bei normalem Betrieb muss die E/A-Ansprechzeit bei der Reaktionszeit nicht berücksichtigt werden. Auch beim Auftreten von Fehlern in Geräten oder dem Netzwerk erfolgt die Abschaltung der Ausgänge innerhalb der Reaktionszeit.

9-4-2 Berechnung der Reaktionszeit

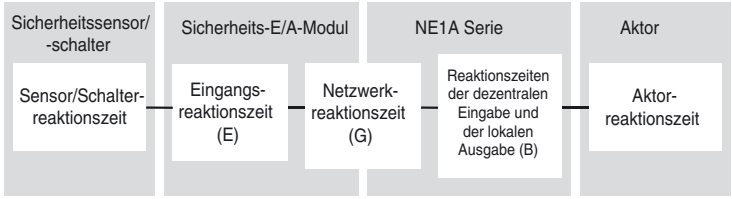
Komponenten der Reaktionszeit

Im Folgenden finden Sie eine Aufstellung der die Reaktionszeit bestimmenden Komponenten für die vier verschiedenen Arten von Sicherheitsketten.

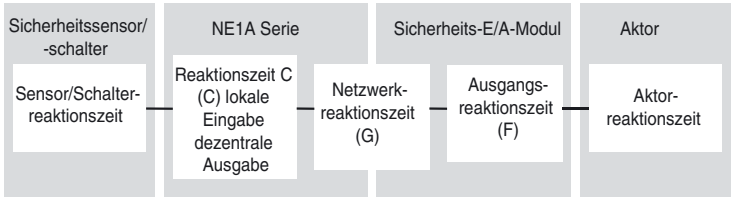
1. Lokale Eingabe / Lokale Ausgabe



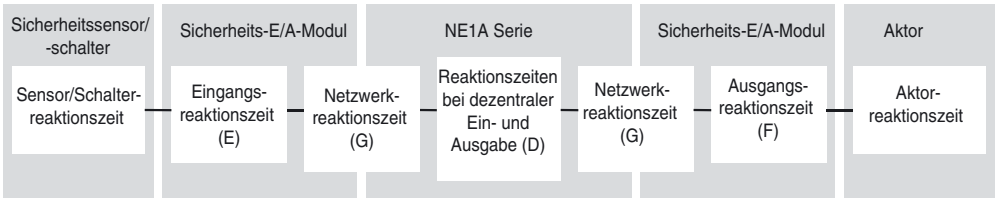
2. Dezentrale Eingabe / Lokale Ausgabe



3. Lokale Eingabe / Dezentrale Ausgabe



4. Dezentrale Eingabe / Dezentrale Ausgabe



Reaktionszeitberechnung

	Parameter	Formel
A	Reaktionszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 bei lokaler Ein- und Ausgabe (ms)	= Ein-/Ausschaltverzögerungszeit + E/A-Aktualisierungszykluszeit + 2 × Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 + 2,5
B	Reaktionszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 bei dezentraler Eingabe und lokaler Ausgabe (ms)	= Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 + 2,5
C	Reaktionszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 bei lokaler Eingabe und dezentraler Ausgabe (ms)	= Ein-/Ausschaltverzögerungszeit + E/A-Aktualisierungszykluszeit + 2 × Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01
D	Reaktionszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 bei dezentraler Ein- und Ausgabe (ms)	= Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01
E	Eingangsreaktionszeit des Sicherheits-E/A-Moduls (ms)	= Ein-/Ausschaltverzögerungszeit + Eingangsreaktionszeit
F	Ausgangsreaktionszeit des Sicherheits-E/A-Moduls (ms)	= Ausgangsreaktionszeit
G	Netzwerkreaktionszeit (ms)	= Ergebnis der Berechnung des Netzwerkkonfigurators

Hinweis Wird der Ausgang eines Funktionsblocks zur Eingangsseite desselben Funktionsblocks zurückgeführt, muss die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A zur Reaktionszeit der Sicherheitskette hinzuaddiert werden.

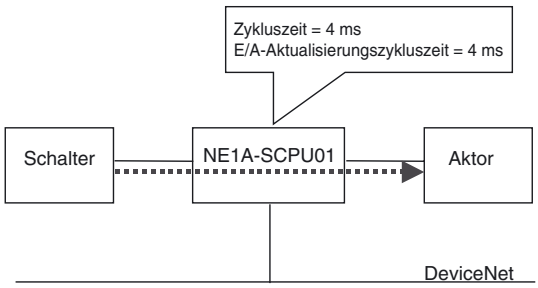
Beispielberechnungen der Reaktionszeit

■ **Beispiel 1: Lokale Eingabe / Lokale Ausgabe**

Das folgende Beispiel zeigt, wie die Reaktionszeit zwischen einer lokalen Eingabe und einer lokalen Ausgabe bei der abgebildeten NE1A-SCPU01 Konfiguration berechnet wird.

NE1A-SCPU01 Konfiguration:

- Programm: 1 AND (2 Eingänge)
- Standard-Slaves: 2 Verbindungen
- Sicherheits-Master: --
- Sicherheits-Slaves: --



Die vom Netzwerkkonfigurator gelesenen Zykluszeiten ergeben sich wie folgt:

Controller-Zykluszeit = 4 ms

E/A-Aktualisierungszykluszeit = 4 ms

Die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU02 beträgt 6 ms, die E/A-Aktualisierungszeit 6 ms.

Die Reaktionszeit wird mit der folgenden Gleichung ermittelt:

Reaktionszeit (ms) = Schalterreaktionszeit

+ Reaktionszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 bei lokaler Ein- und Ausgabe
+ Aktorreaktionszeit = Schalterreaktionszeit
+ Ein-/Ausschaltverzögerungszeit (NE1A-SCPU01) + 4 + 4 × 2 + 2,5
+ Aktorreaktionszeit

= **14,5 + Ein-/Ausschaltverzögerungszeit (Sicherheitsnetzwerk-Controller NE1A)**
+ Schalterreaktionszeit + Aktorreaktionszeit

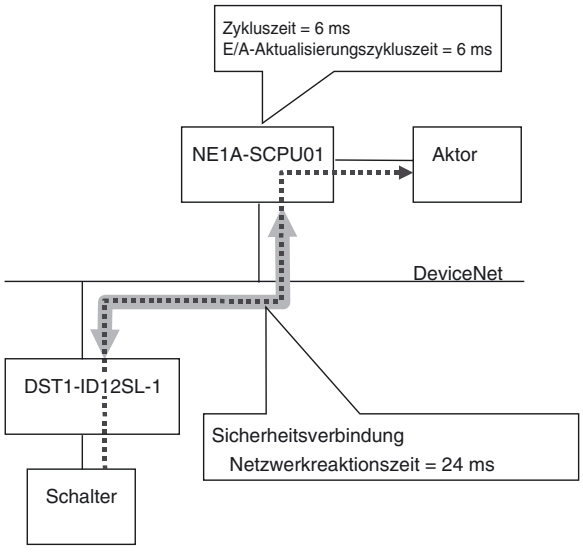
Hinweis Das obige Beispiel 1 zeigt die Konfiguration zur Minimierung der Reaktionszeit des Sicherheitsnetzwerk-Controllers NE1A. Als Richtwert für die Mindestreaktionszeit der Ausführung NE1A-SCPU01(-V1) können 15 ms angenommen werden, bei der Ausführung NE1A-SCPU02 sind es 21 ms. Wenn das Anwendersystem eine kürzere Reaktionszeit erfordert, kann der Controller nicht eingesetzt werden.

■ Beispiel 2: Dezentrale Eingabe / Lokale Ausgabe

Das folgende Beispiel zeigt, wie die Reaktionszeit zwischen einer dezentralen Eingabe und einer lokalen Ausgabe bei der abgebildeten NE1A-SCPU01 Konfiguration berechnet wird.

NE1A-SCPU01 Konfiguration:

- Programm: 1 Safety Gate Monitor, 1 Reset, 1 E-STOP, 1 AND, 1 External Device Monitor
- Standard-Slaves: 2 Verbindungen
- Sicherheits-Master: 1 Verbindung (EPI = 6 ms)
- Sicherheits-Slaves: --



Die vom Netzwerkkonfigurator gelesenen Zykluszeiten ergeben sich wie folgt:

Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 = 6 ms

E/A-Aktualisierungszykluszeit = 6 ms

Die Netzwerkreaktionszeit beträgt 24 ms bei einem Sicherheitsverbindungs-EPI von 6 ms. Die Reaktionszeit wird mit der folgenden Gleichung ermittelt:

Reaktionszeit (ms) = Schalterreaktionszeit
+ Eingangsreaktionszeit des Sicherheits-E/A-Moduls
+ Netzwerkreaktionszeit
+ Reaktionszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 bei dezentraler Eingabe und lokaler Ausgabe
+ Aktorreaktionszeit
= Schalterreaktionszeit
+ Ein-/Ausschaltverzögerung (Sicherheits-E/A-Modul DST1-ID12SL-1) + 16,2
(= Eingangsreaktionszeit des Sicherheits-E/A-Moduls DST1-ID12SL-1)
+ 24
+ 6 + 2.5
+ Aktorreaktionszeit
= **48,7 + Ein-/Ausschaltverzögerungszeit (DST1-ID12SL-1) + Schalterreaktionszeit + Aktorreaktionszeit**

■ **Beispiel 3: Lokale Eingabe / Dezentrale Ausgabe**

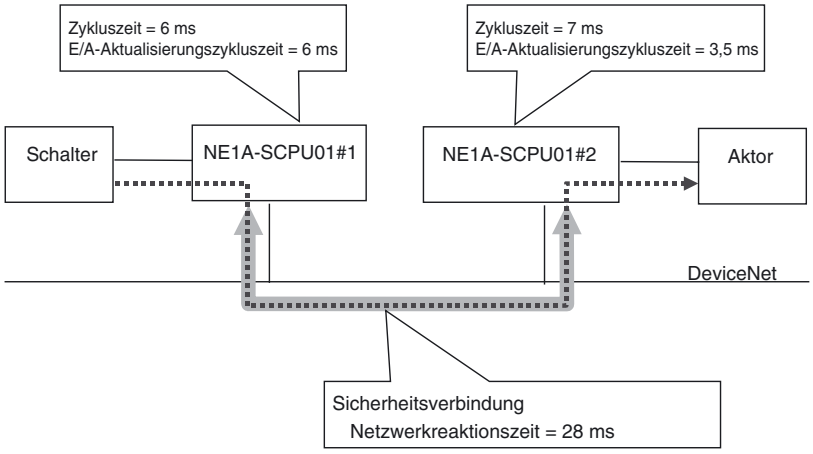
Das folgende Beispiel zeigt, wie die Reaktionszeit zwischen einer lokalen Eingabe und einer dezentralen Ausgabe bei der abgebildeten NE1A-SCPU01 Konfiguration (Knoten 1 und Knoten 2) berechnet wird.

Konfiguration NE1A-SCPU01, Knoten 1 (#1):

- Programm: 1 Safety Gate Monitor, 1 Reset, 1 E-STOP, 1 AND, 1 External Device Monitor
- Standard-Slaves: 2 Verbindungen
- Sicherheits-Master: --
- Sicherheits-Slave: 1 Verbindung (EPI = 7 ms)

Konfiguration NE1A-SCPU01, Knoten 2 (#2):

- Programm: 1 Safety Gate Monitor, 1 Reset, 1 E-STOP, 1 AND, 1 External Device Monitor
- Standard-Slaves: 2 Verbindungen
- Sicherheits-Master: 3 Verbindungen (EPI = 7 ms)
- Sicherheits-Slaves: --



Die vom Netzwerkkonfigurator gelesenen Zykluszeiten für den Knoten 1 (#1) ergeben sich wie folgt:

Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 = 6 ms

E/A-Aktualisierungszykluszeit = 6 ms

Die Zykluszeiten für den Knoten 2 (#2) ergeben sich wie folgt:

Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 = 7 ms

E/A-Aktualisierungszykluszeit = 3,5 ms

Die Netzwerkreaktionszeit beträgt 28 ms bei einem Sicherheitsverbindungs-EPI von 7 ms. Die Reaktionszeit wird mit der folgenden Gleichung ermittelt:

Reaktionszeit (ms) = Schalterreaktionszeit

+ Reaktionszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 Nr. 1 bei lokaler Eingabe und dezentraler Ausgabe

+ Netzwerkreaktionszeit

+ Reaktionszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 Nr. 2 bei dezentraler Eingabe und lokaler Ausgabe

+ Aktorreaktionszeit

= Schalterreaktionszeit

+ Ein-/Ausschaltverzögerungszeit (NE1A-SCPU01) + 6 + 6 × 2

+ 28

+ 7 + 2.5

+ Aktorreaktionszeit

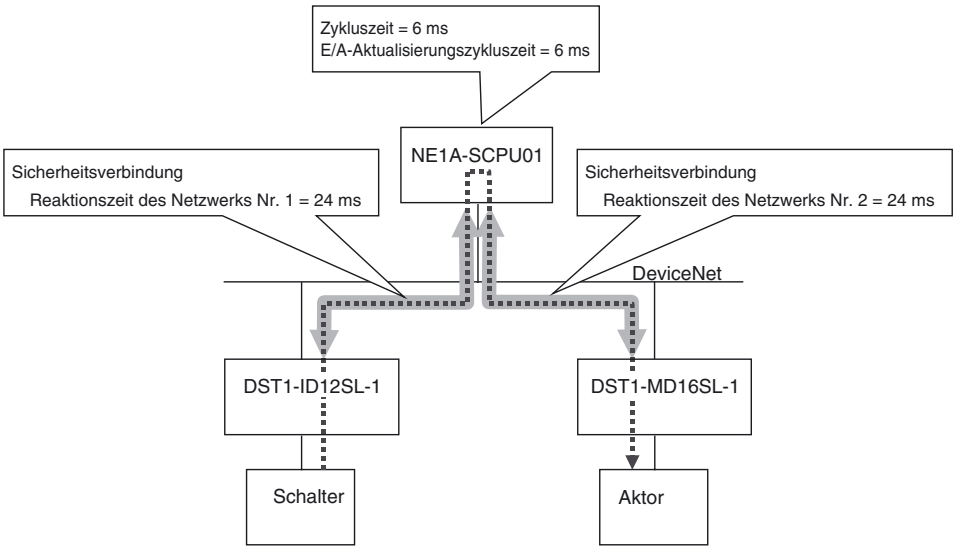
=55,5 + Ein-/Ausschaltverzögerungszeit (NE1A-SCPU01) + Schalterreaktionszeit + Aktorreaktionszeit

■ **Beispiel 4: Dezentrale Eingabe / Dezentrale Ausgabe**

Das folgende Beispiel zeigt, wie die Reaktionszeit zwischen einer dezentralen Eingabe und einer dezentralen Ausgabe bei der abgebildeten NE1A-SCPU01 Konfiguration berechnet wird.

NE1A-SCPU01 Knotenkonfiguration:

- Programm: 1 Reset, 1 E-STOP, 1 External Device Monitor
- Standard-Slaves: 2 Verbindungen
- Sicherheits-Master: 3 Verbindungen (EPI = 6 ms)
- Sicherheits-Slaves: --



Die vom Netzwerkkonfigurator gelesenen Zykluszeiten ergeben sich wie folgt:

Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 = 6 ms

E/A-Aktualisierungszykluszeit = 6 ms

Die Netzwerkreaktionszeiten #1 und #2 betragen jeweils 24 ms bei einem Sicherheitsverbindungs-EPI von 6 ms. Die Reaktionszeiten werden mit der folgenden Gleichung ermittelt:

Reaktionszeit (ms) = Schalterreaktionszeit

+ Eingangsreaktionszeit des Sicherheits-E/A-Moduls

+ Reaktionszeit des Netzwerks Nr. 1

+ Reaktionszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 bei dezentraler Ein- und Ausgabe

+ Reaktionszeit des Netzwerks Nr. 2

+ Ausgangsreaktionszeit des Sicherheits-E/A-Moduls

+ Aktorreaktionszeit

= Schalterreaktionszeit

+ Ein-/Ausschaltverzögerung (Sicherheits-E/A-Modul DST1-ID12SL-1) + 16,2

(= Eingangsreaktionszeit des Sicherheits-E/A-Moduls DST1-ID12SL-1)

+ 24

+ 6

+ 24

+ 6,2 (= Ausgangsreaktionszeit des Sicherheits-E/A-Moduls DST1-MD16SL-1)

+ Aktorreaktionszeit

= **76,4 + Ein-/Ausschaltverzögerungszeit (DST1-ID12SL-1) + Schalterreaktionszeit + Aktorreaktionszeit**

9-4-3 Überprüfung der Reaktionszeit

Bei einer Änderung der Komponenten der Sicherheitssteuerung muss die Reaktionszeit neu berechnet und kontrolliert werden, dass diese noch den Anforderungen an das System genügt. Sollte die neu berechnete Reaktionszeit die Systemanforderungen nicht erfüllen, müssen die Auslegung des Sicherheitsnetzwerks einer kritischen Prüfung unterzogen und entsprechende Konzeptänderungen vorgenommen werden. Hierbei haben sich folgende Maßnahmen als hilfreich erwiesen:

- Durch eine Verkürzung des EPIs kann die Netzwerkreaktionszeit verkürzt werden. Diese Maßnahme führt jedoch auch zu einer Reduzierung der für andere Verbindungen zur Verfügung stehenden Netzwerkbandbreite.
- Die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A wird ausgehend von der Programmgröße, der Anzahl der Verbindungen und weiterer Faktoren automatisch berechnet. Sicherheitsketten, die eine schnellere Reaktionszeit erfordern, können unter Verwendung eines separaten Sicherheitsnetzwerk-Controllers NE1A realisiert werden.

ABSCHNITT 10
Fehlersuche

10-1 Fehlerkategorien 200
10-2 Ermittlung des Fehlerzustands 201
10-3 Anzeige-/Displaystatus und Abhilfemaßnahmen beim Auftreten von Fehlern 202
10-4 Fehlerprotokoll 207
10-4-1 Fehlerprotokolltabelle 207
10-4-2 Fehlerinformationen im Detail 209
10-5 Fehler beim Herunterladen 212
10-5-1 Übersicht 212
10-5-2 Fehlermeldungen und Abhilfemaßnahmen 212
10-6 Fehler beim Zurücksetzen 215
10-6-1 Übersicht 215
10-6-2 Fehlermeldungen und Abhilfemaßnahmen 215
10-7 Fehler beim Wechsel des Betriebsmodus 216
10-7-1 Übersicht 216
10-7-2 Fehlermeldungen und Abhilfemaßnahmen 216
10-8 Verbindungsstatus-Tabellen 217
10-8-1 Übersicht 217
10-8-2 Verbindungsstatus für DST1 218
10-8-3 Verbindungsstatus für den Sicherheitsnetzwerk-Controller NE1A (Sicherheits-Slave-Funktion) 220

10-1 Fehlerkategorien

Die beim Sicherheitsnetzwerk-Controller NE1A möglicherweise auftretenden Fehler lassen sich in die folgenden drei Kategorien unterteilen:

Geringfügige Fehler

Beim Auftreten eines geringfügigen Fehlers an einer lokalen oder einer über eine Sicherheitsverbindung angeschlossenen E/A-Klemme wird diese gestoppt und in den Sicherheitszustand versetzt. Der Controller setzt jedoch den Betrieb fort.

Abbruchfehler

Beim Auftreten eines Abbruchfehlers stoppt der Sicherheitsnetzwerk-Controller NE1A die Sicherheitsfunktionen und versetzt sie in den Sicherheitszustand. Zur Überprüfung des Fehlerzustands werden die Explicit Message-Kommunikation sowie ein Teil der Netzwerkkonfigurator-Funktionen weiterhin unterstützt.

Kritische Fehler

Beim Auftreten eines kritischen Fehlers stoppt der Sicherheitsnetzwerk-Controller NE1A seine Funktionen vollständig.

Hinweis Informationen zu den bei der Konfiguration möglicherweise auftretenden Einstellungsfehlern finden Sie unter *10-5 Fehler beim Herunterladen*.

Hinweis Informationen zu den beim Zurücksetzen möglicherweise auftretenden Fehlern finden Sie unter *10-6 Fehler beim Zurücksetzen*.

Hinweis Informationen zu den beim Betriebsmoduswechsel möglicherweise auftretenden Fehlern finden Sie unter *10-7 Fehler beim Wechseln des Betriebsmodus*.

10-2 Ermittlung des Fehlerzustands

Detailinformationen zu aufgetretenen Fehlern bieten die beiden folgenden Informationsquellen:

- Die LED-Kontrollleuchten an der Front des Sicherheitsnetzwerk-Controllers NE1A
- Das mit dem Netzwerkkonfigurator auslesbare Fehlerprotokoll des Sicherheitsnetzwerk-Controllers NE1A

10-3 Anzeige-/Displaystatus und Abhilfemaßnahmen beim Auftreten von Fehlern

Kritische Fehler

LED-Kontrollleuchten			Fehlerprotokoll		Ursache	Abhilfemaßnahmen
MS	NS	Sieben-segment-anzeige	Eintrag	Speicherung im nichtflüchtigen Speicher		
■ AUS	■ AUS	AUS	--	Nicht unterstützt	• Störpegel höher als erwartet • Kritischer Hardwarefehler	Schalten Sie die Spannungsversorgung aus und wieder ein, und prüfen Sie die Funktion. Wenn die Störung erneut auftritt, ist der Sicherheitsnetzwerk-Controller NE1A möglicherweise fehlerhaft. • Prüfen Sie auf Störeinflüsse, und ergreifen Sie die zur Behebung erforderlichen Maßnahmen.
Leuchtet rot	■ AUS	Links: H Rechts: ---	System Failure	Es werden so viele Informationen gespeichert wie möglich.	• Sicherheits- oder Testausgang war bereits vor Aufnahme des Betriebs an 24 V DC kurzgeschlossen. • Störpegel höher als erwartet • Kritischer Hardwarefehler	• Prüfen Sie die externe Verdrahtung auf Kurzschluss der Spannungsversorgung an der Ausgangsklemme. • Prüfen Sie auf Störeinflüsse, und ergreifen Sie die zur Behebung erforderlichen Maßnahmen. • Schalten Sie die Spannungsversorgung aus und wieder ein, und prüfen Sie auf Funktion. • Wenn die Störung erneut auftritt, ist der Sicherheitsnetzwerk-Controller NE1A möglicherweise fehlerhaft.

Abbruchfehler

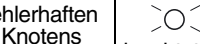
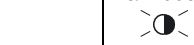
LED-Kontrollleuchten			Fehlerprotokoll		Ursache	Abhilfemaßnahmen
MS	NS	Sieben-segment-anzeige	Eintrag	Speicherung im nichtflüchtigen Speicher		
Blinkt rot	Blinkt grün oder Leuchtet grün	E8 ⇔ Adresse des fehlerhaften Knotens	Schalter Fehl-einstellung	Ja	Die Knotenadresse oder die Baudrate wurden nach erfolgreichem Herunterladen der Konfiguration geändert.	• Stellen Sie die Schalter korrekt ein. • Setzen Sie die Konfigurationsdaten zurück.

Geringfügige Fehler

LED-Kontrollleuchten			Fehlerprotokoll		Ursache	Abhilfemaßnahmen
NS	Sieben-segment-anzeige	E/A-Punke	Eintrag	Speicherung im nichtflüchtigen Speicher		
Leuchtet rot	F0✍ Adresse des fehlerhaften Knotens	---	Duplicate MAC ID	Siehe Hinweis 1.	Knotenadressen-Mehrfachverwendungs-Fehler (mehrere Knoten sind auf dieselbe Knotennummer eingestellt)	Prüfen Sie die Knotenadressen der anderen Knoten. Schalten Sie die Spannungsversorgung aus, beheben Sie den Konfigurationsfehler, und schalten Sie die Spannungsversorgung wieder ein.
Leuchtet rot	F1✍ Adresse des fehlerhaften Knotens	---	Bus OFF	Siehe Hinweis 1.	Bus Off (aufgrund häufiger Datenfehler wurde die Kommunikation deaktiviert)	Schalten Sie die Spannungsversorgung aus, überprüfen Sie die folgenden Punkte, wobei Sie die jeweiligen Abhilfemaßnahmen ergreifen, und schalten Sie die Spannungsversorgung wieder ein. • Stellen Sie sicher, dass die Baudrate aller Knoten auf denselben Wert eingestellt ist. • Stellen Sie sicher, dass die Kabellänge (einschließlich aller Abzweige) die zulässige Maximallänge nicht überschreitet. • Überprüfen Sie alle Kabelverbindungen. • Stellen Sie sicher, dass beide Enden (und nur diese) des Netzwerkstrangs durch Abschlusswiderstände terminiert sind. • Stellen Sie sicher, dass der Störpegel nicht zu hoch ist.

LED-Kontrollleuchten			Fehlerprotokoll		Ursache	Abhilfemaßnahmen
NS	**Sieben-segment-anzeige**	**E/A-Punke**	**Eintrag**	**Speicherung im nichtflüchtigen Speicher**		
Blinkt rot	L9✍ Knoten-adresse des Masters	---	Standard I/O Connection Timeout	Siehe Hinweis 1.	Zeitüberschreitung bei Standard-E/A-Verbindung	Überprüfen Sie die folgenden Punkte: • Stellen Sie sicher, dass die Baudrate aller Knoten auf denselben Wert eingestellt ist. • Stellen Sie sicher, dass die Kabellänge (einschließlich aller Abzweige) die zulässige Maximallänge nicht überschreitet. • Überprüfen Sie alle Kabelverbindungen. • Stellen Sie sicher, dass beide Enden (und nur diese) des Netzwerkstrangs durch Abschlusswiderstände terminiert sind. • Stellen Sie sicher, dass der Störpegel nicht zu hoch ist.
Blinkt rot	dA⇔ Knotenadresse des Ziel-Slaves	---	Safety I/O Connection Timeout	Siehe Hinweis 1.	Zeitüberschreitung bei Sicherheits-E/A-Verbindung	
Blinkt rot	d5⇔ Knoten-adresse des Ziel-Slaves	---	Nonexistent Slave Device	Siehe Hinweis 1.	Slave kann nicht gefunden werden	
Blinkt rot	d6⇔ Knoten-adresse des Ziel-Slaves	---	Safety I/O Connection Establish-ment Failure	Siehe Hinweis 1.	Fehler bei der Einrichtung der Sicherheits-E/A-Verbindung	Überprüfen Sie das Slave-Gerät • Stellen Sie sicher, dass es ordnungsgemäß konfiguriert ist. • Stellen Sie sicher, dass es sich im normalen Betriebszustand befindet.
Blinkt rot	d6⇔ Knoten-adresse des Ziel-Slaves	---	Invalid Slave Device	Siehe Hinweis 1.	Ungültiges Slave-Gerät (Verifizierungs-fehler)	Verifizieren Sie das Slave-Gerät (***Device - Parameters - Compare***), und stellen Sie eine Verbindung zu einem geeigneten Slave-Gerät her.
AUS	E0⇔ Adresse des fehlerhaften Knotens	---	Network PS Voltage Low	Siehe Hinweis 1.	Netzwerkspan-nungsversor-gungsfehler	Überprüfen Sie die folgenden Punkte: • Stellen Sie sicher, dass die Versorgungsspannung innerhalb des vorgesehenen Bereichs liegt. • Überprüfen Sie alle Kabelverbindungen.
---	E2⇔ Adresse des fehlerhaften Knotens	---	Transmission Timeout	Siehe Hinweis 1.	Zeitüberschreitung bei der Übertragung	Überprüfen Sie die folgenden Punkte: • Stellen Sie sicher, dass die Baudrate aller Knoten auf denselben Wert eingestellt ist. • Stellen Sie sicher, dass die Kabellänge (einschließlich aller Abzweige) die zulässige Maximallänge nicht überschreitet. • Überprüfen Sie alle Kabelverbindungen. • Stellen Sie sicher, dass beide Enden (und nur diese) des Netzwerkstrangs durch Abschlusswiderstände terminiert sind. • Stellen Sie sicher, dass der Störpegel nicht zu hoch ist.
Blinkt rot	A0⇔ Adresse des fehlerhaften Knotens	---	Kommuni-kation der jeweiligen Sicherheits-E/A angehal-ten wegen Sicherheits-E/A-Kommu-nikationsfeh-ler	Ja (Siehe Hinweis 2)	Zeitüberschrei-tung einer Sicherheits-E/A-Verbindung mit Unterbrechung der jeweiligen E/A-Verbindung	Überprüfen Sie die folgenden Punkte: • Stellen Sie sicher, dass die Baudrate aller Knoten auf denselben Wert eingestellt ist. • Stellen Sie sicher, dass die Kabellänge (einschließlich aller Abzweige) die zulässige Maximallänge nicht überschreitet. • Überprüfen Sie alle Kabelverbindungen. • Stellen Sie sicher, dass beide Enden (und nur diese) des Netzwerkstrangs durch Abschlusswiderstände terminiert sind. • Stellen Sie sicher, dass der Störpegel nicht zu hoch ist.
Blinkt rot	A1⇔ Adresse des fehlerhaften Knotens	---	Kommuni-kation aller Sicherheits-E/A angehalten wegen Sicherheits-E/A-Kommuni-kationsfehler	Ja (Siehe Hinweis 2)	Zeitüberschrei-tung einer Sicherheits-E/A-Verbindung mit Unterbrechung der jeweiligen E/A-Verbindung	

LED-Kontrollleuchten			Fehlerprotokoll		Ursache	Abhilfemaßnahmen
NS	**Sieben-segment-anzeige**	**E/A-Punke**	**Eintrag**	**Speicherung im nichtflüchtigen Speicher**		
---	P1⇔ Adresse des fehlerhaften Knotens	Klemme ☼ leuchtet rot Klemmen-paar (Zweika-nalmodus) ◑ blinkt rot	External Test Signal Failure at Safety Input	Siehe Hinweis 1.	Fehler in der externen Verdrahtung eines Sicherheits-eingangs	Überprüfen Sie die folgenden Punkte: • Stellen Sie sicher, dass die Eingangssignalleitung keine Verbindung zur Versorgungsspannung hat. • Stellen Sie sicher, dass die Eingangssignalleitung keinen Kontakt zur Masse hat. • Stellen Sie sicher, dass die Eingangssignalleitung nirgendwo unterbrochen ist. • Stellen Sie sicher, dass kein Kurzschluss zwischen Eingangssignalleitungen vorliegt. • Stellen Sie sicher, dass die angeschlossenen Geräte einwandfrei funktionieren. • Stellen Sie sicher, dass die Diskrepanzzeit (Einstellung „Discrepancy Time“) auf einen gültigen Wert eingestellt ist. Zur Aufhebung dieses Fehlerzustands müssen die folgenden Bedingungen erfüllt sein: Die Fehlerhaltezeit muss abgelaufen sein. Die Ursache des Fehlers muss beseitigt worden sein. Die Sicherheitseingangsklemmen müssen auf AUS gesetzt worden sein. Eine Änderung der Diskrepanzzeit erfordert eine Neukonfiguration.
---	P1⇔ Adresse des fehlerhaften Knotens	Klemme eines Klemmen-paares (Zweika-nalmodus) ☼ leuchtet rot	Discrepancy Error at Safety Input	Siehe Hinweis 1.	Diskrepanzfehler zwischen zwei im Zweikanalmodus betriebenen Sicherheits-eingängen	
---	P1⇔ Adresse des fehlerhaften Knotens	Ziel-klemme leuchtet rot ☼ Klemmen-paar (Zweika-nalmodus) ◑ blinkt rot	Internal Input Failure at Safety Input	Siehe Hinweis 1.	Interner Fehler in einem Sicherheits-eingangs-schaltkreis	
---	P2⇔ Adresse des fehlerhaften Knotens	--	Overload Detected at Test Output	Siehe Hinweis 1.	Überlastung eines Testaus-gangs (bei Verwendung des Testausgangs als Standardsignal-ausgang)	Stellen Sie sicher, dass bei der Testausgangssignalleitung kein Erdschluss und keine Überlastung vorliegt.
---	P2⇔ Adresse des fehlerhaften Knotens	--	Stuck-at-high Detected at Test Output	Siehe Hinweis 1.	Der Testaus-gang ist dauerhaft auf EIN gesetzt (bei Verwendung des Testausgangs als Standardsignal-ausgang)	Stellen Sie sicher, dass die Ausgangssignalleitung keinen Kontakt zur Versorgungsspannung hat. Zum Aufheben des Fehlerzustands setzen Sie den Eingang nach Ablauf der Fehlerhaltezeit auf AUS, nachdem Sie die Ursache des Fehlers beseitigt haben. Wenn kein Fehler in der Verdrahtung vorliegt, muss der Sicherheits-netzwerk-Controller NE1A-SCPU01 ausgetauscht werden.
--	P2⇔ Adresse des fehlerhaften Knotens	--	Under Current Detected Using Muting Lamp	Siehe Hinweis 1.	Unterbrechung der Leitung vom Testausgang Muting-Lampe festgestellt (bei Verwendung des Testausgangs T3 als Signalaus-gang für eine Muting-Lampe)	Stellen Sie sicher, dass keine Unterbrechungen der Ausgangssignalleitung vorliegen. Wenn kein Fehler vorliegt, muss die Muting-Lampe überprüft werden.

LED-Kontrollleuchten			Fehlerprotokoll		Ursache	Abhilfemaßnahmen
NS	**Sieben-segment-anzeige**	**E/A-Punke**	**Eintrag**	**Speicherung im nichtflüchtigen Speicher**		
---	P3⇔ Adresse des fehlerhaften Knotens	Ziel-klemme  leuchtet rot Klemmen-paar (Zweika-nalmodus)  blinkt rot	Over Current Detected at Safety Output	Siehe Hinweis 1.	An einem Sicher-heitsausgang wurde ein Über-strom festgestellt	Überprüfen Sie die folgenden Punkte: • Stellen Sie sicher, dass der Sicherheits-ausgang nicht überlastet ist. • Stellen Sie sicher, dass die Ausgangssi-gnalleitung keinen Kontakt zur Masse hat. • Stellen Sie sicher, dass die Ausgangssi-gnalleitung keine Verbindung zur Versor-gungsspannung hat. • Stellen Sie sicher, dass kein Kurzschluss zwischen Ausgangssignalleitungen vorliegt. Zur Aufhebung dieses Fehlerzustands müssen die folgenden Bedingungen erfüllt sein: Die Fehlerhaltezeit muss abgelaufen sein. Die Ursache des Fehlers muss beseitigt worden sein. Das Ausgangssignal für den betroffenen Sicherheitsausgang muss durch die Benut-zeranwendung auf AUS gesetzt worden sein.
---	P3⇔ Adresse des fehlerhaften Knotens	Ziel-klemme leuchtet rot Klemmen-paar (Zweika-nalmodus) blinkt rot	Short Circuit Detected at Safety Output	Siehe Hinweis 1.	An einem Sicher-heitsausgang wurde ein Kurz-schluss erkannt	
---	P3⇔ Adresse des fehlerhaften Knotens	Ziel-klemme leuchtet rot Klemmen-paar (Zweika-nalmodus) blinkt rot	Stuck-at-high Detected at Safety Output	Siehe Hinweis 1.	Der Sicherheits-ausgang ist dau-erhaft auf EIN gesetzt	
---	P3⇔ Adresse des fehlerhaften Knotens	Ziel-klemme leuchtet rot Klemmen-paar (Zweika-nalmodus) blinkt rot	Cross Connection Detected at Safety Output	Siehe Hinweis 1.	Querschluss zwischen Sicher-heitsausgangs-leitungen erkannt	
---	P3⇔ Adresse des fehlerhaften Knotens	Klemme eines Klemmen-paares (Zweika-nalmodus) leuchtet rot	Dual Channel Violation at Safety Output	Siehe Hinweis 1.	An einem Sicher-heitsausgang wurde ein Aus-gangsdaten-fehler erkannt	Überprüfen Sie, ob die Ausgangsdaten des Programms für die beiden im Zweikanal-modus betriebenen Ausgänge als äquiva-lente Kanäle konfiguriert sind.

LED-Kontrollleuchten			Fehlerprotokoll		Ursache	Abhilfemaßnahmen
NS	**Sieben-segment-anzeige**	**E/A-Punke**	**Eintrag**	**Speicherung im nichtflüchtigen Speicher**		
---	P4⇔ Adresse des fehlerhaften Knotens	● Alle AUS	Input PS Voltage Low	Siehe Hinweis 1.	Es wird eine Sicherheits-Eingangs- oder Testausgangs-Klemme verwendet, jedoch ist die Eingangs-Versorgungsspannung nicht angeschlossen oder nicht eingeschaltet.	Überprüfen Sie die folgenden Punkte: • Stellen Sie sicher, dass die Versorgungsspannung innerhalb des vorgesehenen Bereichs liegt. • Überprüfen Sie alle Kabelverbindungen.
---	P5⇔ Adresse des fehlerhaften Knotens	● Alle AUS	Output PS Voltage Low	Siehe Hinweis 1.	Es wird eine Sicherheits-Ausgangs-Klemme verwendet, jedoch ist die Ausgangs-Versorgungsspannung nicht angeschlossen oder nicht eingeschaltet.	

Hinweis (1) Speicherung nur bei Controllern ab Version 1.0.

(2) Diese Funktionen werden nicht von Controllern vor Version 1.0 unterstützt. Die Fehlerdaten werden von Controllern ab Version 1.0 gespeichert.

10-4 Fehlerprotokoll

Im Fehlerprotokoll werden alle Fehler aufgezeichnet, die der Sicherheitsnetzwerk-Controller während seiner Gesamtbetriebszeit erkennt.

Das Fehlerprotokoll kann mithilfe des Netzwerkkonfigurators eingesehen werden.

10-4-1 Fehlerprotokolltabelle

Fehlerprotokolltabelle

Bei Erkennung eines Fehlers in einem Sicherheitsnetzwerk-Controller NE1A vor Version 1.0 wird der Fehler in der Fehlerprotokolltabelle im RAM des Controllers gespeichert. Das Fehlerprotokoll enthält einen Eintrag je Fehler und bietet Platz für bis zu 20 Einträge. Wenn das Fehlerprotokoll bereits 20 Einträge enthält, wird der älteste Eintrag gelöscht und die neuen Daten werden gespeichert.

Bei Erkennung eines Fehlers in einem Sicherheitsnetzwerk-Controller 1.0 ab Version NE1A wird der Fehler in der Fehlerprotokolltabelle im RAM des Controllers gespeichert. Das Fehlerprotokoll enthält einen Eintrag je Fehler und bietet Platz für bis zu 100 Einträge. Wenn das Fehlerprotokoll bereits 100 Einträge enthält, wird der älteste Eintrag gelöscht und die neuen Daten werden gespeichert.

Die Einträge in der Fehlerprotokolltabelle enthalten folgende Informationen:

- Statusdaten zum Zeitpunkt des Fehlers
- Zeitpunkt des Fehlers (Gesamtbetriebszeit des Sicherheitsnetzwerk-Controllers NE1A)
- Adresse des Knotens, an dem der Fehler aufgetreten ist, oder Wert der Fehlerrückmeldung (bei Explicit-Message-Übermittlung)

Fehlerprotokollbereich

Die Fehlerprotokolltabelle ist im RAM des Sicherheitsnetzwerk-Controllers NE1A abgelegt. Beim Auftreten eines kritischen Fehlers wird zusätzlich ein Eintrag im nichtflüchtigen Speicher des Sicherheitsnetzwerk-Controllers NE1A angelegt. Das Fehlerprotokoll im nichtflüchtigen Speicher bleibt erhalten, wenn die Versorgungsspannung des Sicherheitsnetzwerk-Controllers ausgeschaltet wird, und wird nach dem Wiedereinschalten der Versorgungsspannung in das RAM des Sicherheitsnetzwerk-Controllers kopiert.
Beim Auslesen des Fehlerprotokolls mithilfe des Netzwerkkonfigurators wird auf das Fehlerprotokoll im RAM zugegriffen. Beim Löschen des Fehlerprotokolls werden jedoch beide Versionen des Fehlerprotokolls (im RAM und im nichtflüchtigen Speicher) gelöscht.

Einsehen und Löschen der Fehlerprotokolltabelle

Das Fehlerprotokoll kann mit Hilfe der Funktion „Error History Display“ des Netzwerkkonfigurators in Echtzeit eingesehen werden. Die Fehlerprotokolldaten können auch auf dem Netzwerkkonfigurator-PC gespeichert werden.

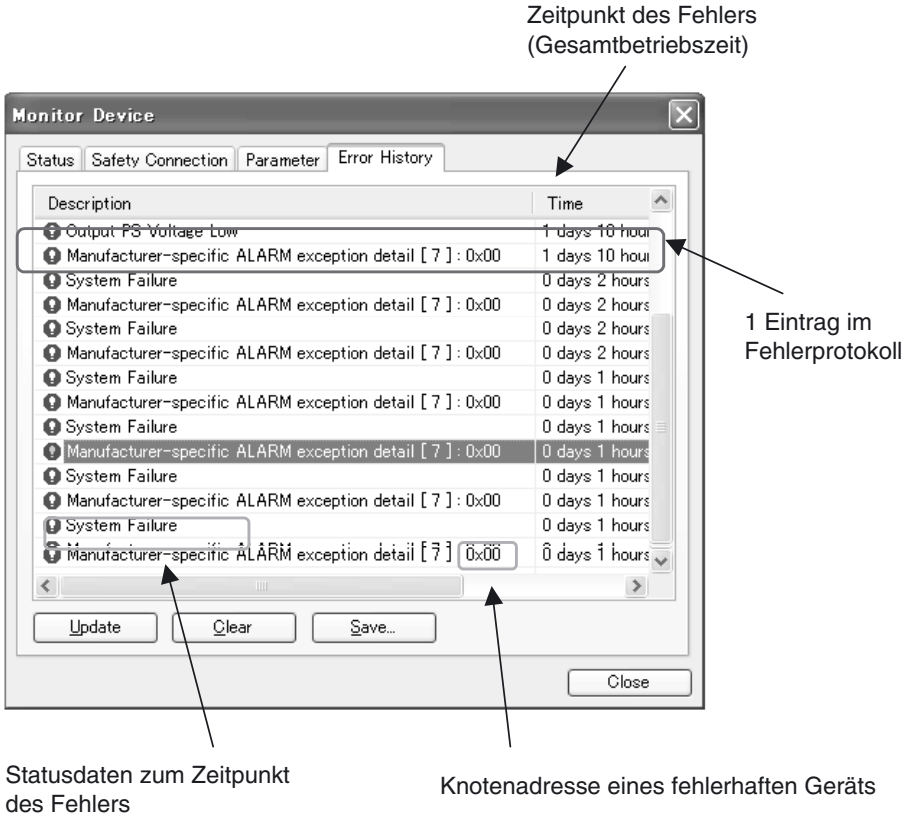
Hinweis

(1) Die Aufzeichnung der Gesamtbetriebszeit des Sicherheitsnetzwerk-Controllers NE1A erfolgt durch Akkumulation (in 6-Minuten-Schritten) der Zeit, in der die Versorgungsspannung der internen Schaltkreise anliegt. Die Gesamtbetriebszeit kann mithilfe des Befehls „Reset“ zurückgesetzt werden.

(2) Beim Auslesen des Fehlerprotokolls mit dem Netzwerkkonfigurator wird die Adresse des Knotens, an dem der Fehler aufgetreten ist, oder der Wert der Rückmeldung als herstellerspezifisches Ausnahmedetail ALARM [7] 0x** angezeigt.

(3) Beim Auslesen des Fehlerprotokolls mit dem Netzwerkkonfigurator werden Fehlerstatusdaten und Adresse des Knotens, an dem der Fehler aufgetreten ist, bzw. Wert der Fehlerrückmeldung für die einzelnen Fehlerprotokolle angezeigt.

Die Fehlerprotokolle des Sicherheitsnetzwerk-Controllers NE1A werden wie folgt mit dem Netzwerkkonfigurator ausgelesen.



10-4-2 Fehlerinformationen im Detail

Meldung		Abhilfemaßnahmen
Systemfehler des Sicherheitsnetzwerk-Controllers NE1A		
System Failure	Systemfehler	Wenn der Systemfehler nach dem Ausschalten und Wiedereinschalten der Versorgungsspannung weiterhin besteht, muss der Sicherheitsnetzwerk-Controller NE1A-SCPU01 ausgetauscht werden.
Invalid Configuration	Ungültige Konfiguration	Die Konfiguration weicht von der ursprünglichen Konfiguration ab. Überprüfen Sie die Konfiguration und konfigurieren Sie den Sicherheitsnetzwerk-Controller NE1A neu.
Fehler in der Logik-Programmierung		
Function Block Status Error	Funktionsblock-Statusfehler	In den Konfigurationsparametern des Funktionsblocks wurde ein unzulässiger Signaleingang als Eingangsbedingung konfiguriert. Überprüfen Sie die in den Funktionsblock eingegebenen Eingänge oder die Programmlogik.
Fehler in der DeviceNet-Kommunikation		
Switch Setting Mismatch	Schalterfehleinstellung	Stellen Sie sicher, dass die Knotenadresse der zuletzt heruntergeladenen Konfiguration entspricht. Ändern Sie ggf. die Einstellung der Knotenadresse oder die Konfiguration. Tritt der Fehler erneut auf, so tauschen Sie den Sicherheitsnetzwerk-Controller NE1A-SCPU01 aus.
Duplicate MAC ID	Mehrfache Verwendung einer Knotenadresse	Prüfen Sie die Knotenadressen der anderen Knoten. Korrigieren Sie die Konfiguration so, dass jede Knotenadresse nur einmal Verwendung findet. Schalten Sie dann die Versorgungsspannung aus und wieder ein.
Network PS Voltage Low	Netzwerkspannungsversorgungsfehler	Überprüfen Sie die folgenden Punkte: • Stellen Sie sicher, dass die Versorgungsspannung innerhalb des vorgesehenen Bereichs liegt. • Überprüfen Sie alle Kabelverbindungen.
Bus Off	Bus Aus (aufgrund häufiger Datenfehler wurde die Kommunikation deaktiviert)	Überprüfen Sie die folgenden Punkte: • Stellen Sie sicher, dass die Baudrate aller Knoten auf denselben Wert eingestellt ist. • Stellen Sie sicher, dass die Kabellänge (einschließlich aller Abzweige) die zulässige Maximallänge nicht überschreitet. • Überprüfen Sie alle Kabelverbindungen. • Stellen Sie sicher, dass beide Enden (und nur diese) des Netzwerkstrangs durch Abschlusswiderstände terminiert sind. • Stellen Sie sicher, dass der Störpegel nicht zu hoch ist. • Stellen Sie sicher, dass der Slave Versorgungsspannung erhält.
Transmission Timeout	Zeitüberschreitung bei der Übertragung	
Standard I/O Connection Timeout	Zeitüberschreitung bei Standard-E/A-Verbindung	
Kommunikation der jeweiligen Sicherheits-E/A angehalten wegen Sicherheits-E/A-Kommunikationsfehler	Die jeweilige Sicherheits-E/A-Verbindung wurde aufgrund einer Zeitüberschreitung angehalten.	
Kommunikation aller Sicherheits-E/A angehalten wegen Sicherheits-E/A-Kommunikationsfehler	Alle Sicherheits-E/A-Verbindung wurden aufgrund einer Zeitüberschreitung angehalten.	
Safety I/O Connection Timeout	Zeitüberschreitung bei Sicherheits-E/A-Verbindung	
Nonexistent Slave Device	Slave kann nicht gefunden werden	
Safety I/O Connection Establishment Failure	Fehler bei der Einrichtung der Sicherheits-E/A-Verbindung	Überprüfen Sie die folgenden Punkte: • Stellen Sie sicher, dass der Sicherheitsnetzwerk-Controller ordnungsgemäß konfiguriert ist. • Stellen Sie sicher, dass der Sicherheitsnetzwerk-Controller normal arbeitet.
Invalid Slave Device	Unbefugtes Slave-Gerät (Verifizierungsfehler)	Verifizieren Sie das Slave-Gerät (***Device - Parameters - Compare***), und stellen Sie eine Verbindung zu einem geeigneten Slave-Gerät her.
EM Transmission Error (Duplicate MAC ID)	Aufgrund der doppelten Verwendung einer Knotenadresse war keine Übertragung möglich	Siehe Abschnitt *Duplicate MAC ID*.
EM Transmission Error (Invalid Header)	Aufgrund eines ungültigen Headers war keine Übertragung möglich	Überprüfen Sie die folgenden Punkte: • Knotenadresse der Nachricht • Klassen-ID der Nachricht • Instanz-ID der Nachricht

Meldung		Abhilfemaßnahmen
Systemfehler des Sicherheitsnetzwerk-Controllers NE1A		
EM Transmission Error (Device Offline)	Eine Übertragung war nicht möglich, da das adressierte lokale Gerät ausgeschaltet oder nicht an das Netzwerk angeschlossen ist.	Überprüfen Sie die folgenden Punkte: • Stellen Sie sicher, dass die Baudrate aller Knoten auf denselben Wert eingestellt ist. • Stellen Sie sicher, dass die Kabellänge (einschließlich aller Abzweige) die zulässige Maximallänge nicht überschreitet. • Überprüfen Sie alle Kabelverbindungen. • Stellen Sie sicher, dass beide Enden (und nur diese) des Netzwerkstrangs durch Abschlusswiderstände terminiert sind. • Stellen Sie sicher, dass der Störpegel nicht zu hoch ist. • Stellen Sie sicher, dass die Versorgungsspannung des Netzwerks innerhalb des vorgesehenen Bereichs liegt.
EM Transmission Error (Message ID Error)	Aufgrund eines Nachrichten-ID-Fehlers war keine Übertragung möglich	
EM Transmission Error (Response Timeout)	Aufgrund einer Zeitüberschreitung beim Warten auf eine Antwort war keine Übertragung möglich	
EM Transmission Error (Destination Device Absence)	Eine Übertragung war nicht möglich, da das adressierte Gerät ausgeschaltet oder nicht an das Netzwerk angeschlossen ist.	Überprüfen Sie die folgenden Punkte: • Zielknotenadresse • Knotenadresse der Nachricht • Stellen Sie sicher, dass die Versorgungsspannung des adressierten Geräts innerhalb des vorgesehenen Bereichs liegt. • Stellen Sie sicher, dass die Baudrate aller Knoten auf denselben Wert eingestellt ist. • Stellen Sie sicher, dass die Kabellänge (einschließlich aller Abzweige) die zulässige Maximallänge nicht überschreitet. • Überprüfen Sie alle Kabelverbindungen. • Stellen Sie sicher, dass beide Enden (und nur diese) des Netzwerkstrangs durch Abschlusswiderstände terminiert sind. • Stellen Sie sicher, dass der Störpegel nicht zu hoch ist.
EM Transmission Error (Destination Buffer Full)	Eine Übertragung war nicht möglich, da der Eingangspuffer des adressierten Geräts die Nachricht nicht aufnehmen konnte	Überprüfen Sie das adressierte Gerät auf die maximal zulässige Länge eingehender Nachrichten.
EM Transmission Error (Command Length Error)	Eine Übertragung war nicht möglich, da die Befehlslänge die maximal zulässige Länge überschreitet	Überprüfen Sie das adressierte Gerät auf die maximal zulässige Länge eingehender Nachrichten. Überprüfen Sie die in der Anforderungsnachricht erwartete Größe der Antwortnachricht.
EM Transmission Error (New Request Received)	Die Nachricht wurde aufgrund des Empfangs der neuen Anforderung gelöscht.	Keine
Received Error Response (UEM)	Empfang einer Fehlerantwort bei Verwendung der anwenderdefinierten Explicit Message-Funktion	Stellen Sie sicher, dass der angegebene Dienst bzw. die Datengröße in der anwenderdefinierten Explicit Message den Spezifikationen des adressierten Geräts entsprechen.
Fehler der E/A-Spannungsversorgung		
Input PS Voltage Low	Die Versorgungsspannung für die Eingänge liegt nicht an	Überprüfen Sie die folgenden Punkte: • Stellen Sie sicher, dass die Versorgungsspannung innerhalb des vorgesehenen Bereichs liegt. • Überprüfen Sie alle Kabelverbindungen.
Output PS Voltage Low	Die Versorgungsspannung für die Ausgänge liegt nicht an	
Fehler der Sicherheitseingänge		
External Test Signal Failure at Safety Input	Fehler der externen Verdrahtung eines Sicherheitseingangs	Überprüfen Sie die folgenden Punkte: • Stellen Sie sicher, dass die Eingangssignalleitung keine Verbindung zur Versorgungsspannung hat. • Stellen Sie sicher, dass die Eingangssignalleitung keinen Kontakt zur Masse hat. • Stellen Sie sicher, dass die Eingangssignalleitung nirgendwo unterbrochen ist. • Stellen Sie sicher, dass kein Kurzschluss zwischen Eingangssignalleitungen vorliegt. • Stellen Sie sicher, dass das angeschlossene Gerät einwandfrei funktioniert. • Stellen Sie sicher, dass die Diskrepanzzeit (Einstellung „Discrepancy Time“) auf einen gültigen Wert eingestellt ist. Zur Aufhebung dieses Fehlerzustands müssen die folgenden Bedingungen erfüllt sein: Die Fehlerhaltezeit muss abgelaufen sein. Die Ursache des Fehlers muss beseitigt worden sein. Die Sicherheitseingangsklemmen müssen auf AUS gesetzt worden sein. Eine Änderung der Diskrepanzzeit erfordert eine Neukonfiguration.
Discrepancy Error at Safety Input	Diskrepanzfehler zwischen zwei im Zweikanalmodus betriebenen Sicherheitseingängen	

Meldung		Abhilfemaßnahmen
Systemfehler des Sicherheitsnetzwerk-Controllers NE1A		
Internal Input Failure at Safety Input	Interner Fehler in einem Sicherheitseingangsschaltkreis	Wenn der Systemfehler nach dem Ausschalten und Wiedereinschalten der Versorgungsspannung weiterhin besteht, muss der Sicherheitsnetzwerk-Controller NE1A-SCPU01 ausgetauscht werden.
Fehler der Testausgänge		
Overload Detected at Test Output	Überlastung des Testausgangs festgestellt	Stellen Sie sicher, dass bei der Testausgangssignalleitung kein Erdschluss und keine Überlastung vorliegt.
Stuck-at-high Detected at Test Output	Der Testausgang ist dauerhaft auf EIN gesetzt	Stellen Sie sicher, dass die Testausgangssignalleitung keinen Kontakt zur Versorgungsspannung hat. Zum Aufheben des Fehlerzustands setzen Sie den Eingang nach Ablauf der Fehlerhaltezeit auf AUS, nachdem Sie die Ursache des Fehlers beseitigt haben. Wenn kein Fehler in der Verdrahtung vorliegt, muss der Sicherheitsnetzwerk-Controller NE1A-SCPU01 ausgetauscht werden.
Under Current Detected Using Muting Lamp	Die Strombelastung des als Muting-Lampen-Ausgang verwendeten Testausgangs hat den unteren Grenzwert unterschritten.	Stellen Sie sicher, dass keine Unterbrechungen der Ausgangssignalleitung vorliegen. Wenn kein Fehler in der Verdrahtung vorliegt, ist möglicherweise die Muting-Lampe defekt.
Fehler der Sicherheitsausgänge		
Over Current Detected at Safety Output	An einem Sicherheitsausgang wurde ein Überstrom festgestellt	Überprüfen Sie die folgenden Punkte: • Stellen Sie sicher, dass der Sicherheitsausgang nicht überlastet ist. • Stellen Sie sicher, dass die Ausgangssignalleitung keinen Kontakt zur Masse hat. • Stellen Sie sicher, dass die Ausgangssignalleitung keine Verbindung zur Versorgungsspannung hat. • Stellen Sie sicher, dass kein Kurzschluss zwischen Ausgangssignalleitungen vorliegt. Zur Aufhebung dieses Fehlerzustands müssen die folgenden Bedingungen erfüllt sein: Die Fehlerhaltezeit muss abgelaufen sein. Die Ursache des Fehlers muss beseitigt worden sein. Das Ausgangssignal für den betroffenen Sicherheitsausgang muss durch die Benutzeranwendung auf AUS gesetzt worden sein.
Short Circuit Detected at Safety Output	An einem Sicherheitsausgang wurde ein Kurzschluss erkannt	
Stuck-at-high Detected at Safety Output	Der Sicherheitsausgang ist dauerhaft auf EIN gesetzt	
Cross Connection Detected at Safety Output	Es wurde ein Querschluss zwischen Sicherheitsausgangsleitungen erkannt	
Dual Channel Violation at Safety Output	An einem Sicherheitsausgang wurde ein Ausgangsdatenfehler erkannt	Überprüfen Sie, ob die Daten für die beiden im Zweikanalmodus betriebenen Ausgänge als äquivalente Kanäle konfiguriert sind.

10-5 Fehler beim Herunterladen

10-5-1 Übersicht

Der Sicherheitsnetzwerk-Controller NE1A oder eine andere Sicherheitseinrichtung kann beim Herunterladen von Konfigurationsdaten Fehlermeldungen generieren. Anhand der vom Netzwerkkonfigurator angezeigten Fehlerinformationen kann die Fehlerursache bestimmt werden.

10-5-2 Fehlermeldungen und Abhilfemaßnahmen

Meldung des Netzwerkkonfigurators	Abhilfemaßnahme
Cannot be executed in the current mode.	Es ist ein kritischer oder ein Abbruchfehler aufgetreten, die LED-Kontrollleuchte MS blinkt rot. Stellen Sie die Schalter korrekt ein, oder führen Sie eine Rücksetzung durch, um die Konfigurationsdaten zu löschen.
The device is locked.	Die Konfigurationsdaten sind gesperrt (LED-Kontrollleuchte LOCK leuchtet). Heben Sie die Sperrung auf
The TUNID is different.	Nach einem Zurücksetzen des Sicherheitsnetzwerk-Controllers wurde die TUNID nicht neu gesetzt (LED-Kontrollleuchte NS blinkt grün/rot), oder die eingestellte TUNID stimmt mit der vom Netzwerkkonfigurator heruntergeladenen TUNID nicht überein. Gehen Sie zur Überprüfung der Einstellung folgendermaßen vor: 1. Setzen Sie den Sicherheitsnetzwerk-Controller NE1A auf die Standardeinstellung zurück. Laden Sie die Parameter dann erneut herunter. Möglicherweise unterscheidet sich die Netzwerknummer von der der übrigen Geräte. Zeigt die Siebensegmentanzeige des Controllers nach dem Wechsel des Betriebsmodus „d6“ an (Meldung *Safety I/O Connection Establishment Failure* erscheint auf der Registerkarte „Error History“ im Fenster „Monitor Device“ des Netzwerkkonfigurators), führen Sie Schritt (2) oder (3) durch, um den Fehler zu beheben. 2. Wählen Sie ***Network – Upload*** im Netzwerkkonfigurator. Vereinheitlichen Sie die Netzwerknummern, und setzen Sie alle Geräte auf die Standardeinstellungen zurück. Laden Sie nach der Rücksetzung erneut die Parameter für alle Geräte. 3. Wählen Sie den Eintrag ***Network – Property***. Darauf hin wird das Dialogfeld „Network Property“ im Netzwerkkonfigurator angezeigt. Klicken Sie im Feld „Network Number“ auf die Schaltfläche **Get from Network**. Wenn mehrere Netzwerknummern vorhanden sind, wählen Sie eine davon aus, und passen Sie die übrigen Nummern daran an.
Privilege violation.	1. Das verwendete Passwort berechtigt nicht zur Änderung der Konfiguration. Überprüfen Sie, ob das korrekte Passwort verwendet wurde.
	2. Es wurde versucht, über eine DeviceNet-Verbindung eine Standalone-Konfiguration in den Sicherheitsnetzwerk-Controller NE1A-SCPU01 herunter zu laden. Schließen Sie den Sicherheitsnetzwerk-Controller über eine USB-Verbindung an den Netzwerkkonfigurator an, und laden Sie die Konfiguration erneut herunter.
Cannot be executed in the current device mode.	Es werden gleichzeitig Daten von mehreren Instanzen des Netzwerkkonfigurators heruntergeladen. Warten Sie, bis andere Downloads abgeschlossen sind.

Meldung des Netzwerkkonfigurators	Abhilfemaßnahme
An error was found during parameter check.	1. Fehlende Übereinstimmung zwischen Konfigurationsparametern. Überprüfen Sie die folgenden Punkte, und ändern Sie ggf. die Parameter. • Ein für einen Funktionsblock gesetzter Zeitparameter (z.B. Discrepancy Time) ist kürzer als die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A. • Das EPI für eine Sicherheitsverbindung ist kürzer als die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A. • Für einen Sicherheitseingang ist der Modus *Used with test pulse* ausgewählt, aber der Parameter „Test Source“ ist nicht eingestellt. • Einer von den beiden für den Zweikanalmodus programmierten Sicherheitseingängen war ein Standardeingang, der andere jedoch nicht. • Einer von den beiden für den Zweikanalmodus programmierten Sicherheitseingängen war auf *Not used* eingestellt, der andere jedoch nicht. • Einer von den beiden für den Zweikanalmodus programmierten Sicherheitsausgängen war auf *Not used* eingestellt, der andere jedoch nicht. • Bei der Sicherheits-E/A-Konfiguration wurde die maximale Anzahl von Verbindungs-IDs für einen Sicherheits-Master (12) überschritten. Ändern Sie die ID-Zuordnung unter ***Edit Safety Connection – Expansion Connection Setting*** zu „Check Produced IDs in the Safety Slave“ in der entsprechenden Sicherheits-E/A-Verbindungseinstellung („Safety Input Assembly“), und laden Sie dann die Geräteparameter erneut in den Sicherheits-Master.
	2. Das Programm wurde möglicherweise mit einer Version des Netzwerkkonfigurators erstellt, die älter ist als Version 1.5□. Die Prüfungen für Sicherheitsfunktionen wurden in Version 1.5□ verbessert, weshalb Programme aus früheren Versionen nicht unverändert heruntergeladen werden können. Gehen Sie wie folgt vor, um das Programm zu konvertieren, und laden Sie es dann erneut herunter. a. Klicken Sie auf der Registerkarte „Logic“ des Fensters „Edit Device Parameters“ des Sicherheitsnetzwerk-Controllers NE1A auf die Schaltfläche **Edit**. b. Wählen Sie ***Edit – Find Function Blocks with Open Connections***, um zu prüfen, ob alle Funktionsblock-E/A verbunden sind. Informationen zu unterbrochenen Funktionsblockverbindungen finden Sie unter *6-3-10 Vorkehrungen beim Wechsel von Version 1.3□ zu 1.5□* im Konfigurationshandbuch *DeviceNet Safety System* (Z905). c. Wählen Sie ***File – Apply*** , um das Logik-Programm zu speichern, und schließen Sie dann den Logik-Editor. d. Wechseln Sie zurück zum Fenster „Edit Device Parameters“ des Sicherheitsnetzwerk-Controllers NE1A, und klicken Sie auf **OK** .
	3. Die Hardware ist möglicherweise fehlerhaft. Schalten Sie die Spannungsversorgung des Sicherheitsnetzwerk-Controllers NE1A aus und wieder ein, und führen Sie eine Selbstdiagnose durch. Wenn Die Anzeige „MS“ rot leuchtet, ersetzen Sie die Hardware.
The data used by the logic program is not aligned with other data.	Die Netzwerkkonfiguration hat sich geändert, sodass die Daten des Logik-Programms nicht mehr mit anderen Daten übereinstimmen. Starten Sie den Logik-Editor, prüfen Sie auf geänderte E/A-Positionen, und nehmen Sie die Einstellungen erneut vor.
Could not access the device.	Das Gerät wartet auf eine TUNID-Einstellung (Kontrollleuchte „NS“ blinkt grün/rot), nachdem während des Downloads eine Rücksetzung über einen anderen Knoten erfolgte. Stellen Sie die TUNID ein und laden Sie die Daten erneut herunter. Informationen zu TUNIDs finden Sie unter *3-4-2 Netzwerknummern* im Konfigurationshandbuch *DeviceNet Safety System* (Z905).
Could not open connection.	1. Während des DeviceNet-Downloads konnte keine Verbindung zum Gerät hergestellt werden. Vergewissern Sie sich, dass die Spannungsversorgung des Geräts eingeschaltet ist, und laden Sie die Daten erneut herunter.
	2. Die für das Gerät verfügbaren Verbindungsressourcen werden für Sicherheits-E/A-Verbindungen mit dem Sicherheits-Master genutzt, sodass ein Verbindungsaufbau zum Netzwerkkonfigurator nicht möglich ist. Ändern Sie den Betriebsmodus des Sicherheits-Masters, für den die Sicherheitsverbindungen registriert sind, zu IDLE.
	3. Möglicherweise wurde die Kommunikation auch durch einen hohen Störpegel oder andere Faktoren beeinträchtigt. Prüfen Sie die folgenden Punkte. • Haben alle Knoten dieselbe Baudrate? • Stimmen die Kabellängen (Sammel- und Abzweigleitungen)? • Ist das Kabel unterbrochen oder lose? • Sind die beiden Enden (und nur diese) des Netzwerkstrangs durch Abschlusswiderstände terminiert?

Meldung des Netzwerkkonfigurators	Abhilfemaßnahme
Message could not be sent.	Beim Herunterladen über USB konnte keine Verbindung zum Gerät hergestellt werden. Vergewissern Sie sich, dass die Spannungsversorgung des Geräts eingeschaltet ist, und laden Sie die Daten erneut herunter.
Connection failed.	Verbindungsfehler beim Versuch, ein Gerät im DeviceNet Netzwerk über die USB-Schnittstelle des Sicherheitsnetzwerk-Controllers NE1A zu konfigurieren. Vergewissern Sie sich, dass die Spannungsversorgung des Geräts eingeschaltet ist, und laden Sie die Daten erneut herunter. Möglicherweise wurde die Kommunikation auch durch einen hohen Störpegel oder andere Faktoren beeinträchtigt. Prüfen Sie die folgenden Punkte. • Haben alle Knoten dieselbe Baudrate? • Stimmen die Kabellängen (Sammel- und Abzweigleitungen)? • Ist das Kabel unterbrochen oder lose? • Sind die beiden Enden (und nur diese) des Netzwerkstrangs durch Abschlusswiderstände terminiert? • Gibt es einen hohen Störpegel?
Program incomplete. Start Logic Editor and check program.	Es gibt unterbrochene Ein- oder Ausgänge in einem vom Logik-Programm genutzten Funktionsblock. Klicken Sie auf der Registerkarte „Logic“ auf die Schaltfläche **Edit** , um die Logik zu öffnen, und gehen Sie wie folgt vor: • Verbinden Sie die unterbrochenen Ein- oder Ausgänge. • Ändern Sie die für den Funktionsblock eingestellte E/A-Anzahl, um den unterbrochenen Ein- oder Ausgang zu löschen. Funktionsblöcke mit unterbrochenen Ein- oder Ausgängen können mit ***Edit – Find Function Blocks with Open Connections*** gesucht werden Informationen zu unterbrochenen Funktionsblockverbindungen finden Sie unter *6-3-10 Vorkehrungen beim Wechsel von Version 1.3□ zu 1.5□* im Konfigurationshandbuch *DeviceNet Safety System* (Z905).

10-6 Fehler beim Zurücksetzen

10-6-1 Übersicht

Der Sicherheitsnetzwerk-Controller NE1A kann beim Zurücksetzen Fehlermeldungen generieren.
Anhand der vom Netzwerkkonfigurator angezeigten Meldungen kann die Fehlerursache identifiziert und der Fehler behoben werden.

10-6-2 Fehlermeldungen und Abhilfemaßnahmen

Meldung des Netzwerkkonfigurators	Abhilfemaßnahmen
Cannot execute in current mode.	Der spezifizierte Rücksetzvorgang kann im aktuellen Betriebsmodus bzw. Zustand des Geräts nicht ausgeführt werden Siehe Abschnitt *7-2-2 Rücksetzvarianten und Zustand des Sicherheitsnetzwerk-Controllers NE1A*. Ändern Sie den Betriebsmodus, oder heben Sie den Konfigurationsschutz des Controllers auf. Führen Sie dann die Rücksetzung erneut aus.
The device has a different TUNID. The device TUNID will be used to reset. Is that OK?	Die im Sicherheitsnetzwerk-Controller NE1A gespeicherte TUNID entspricht nicht der im Netzwerkkonfigurator festgelegten TUNID. Vergewissern Sie sich, dass die Knotenadresse des Geräts übereinstimmt, und führen Sie die Rücksetzung aus, wenn die Verwendung der Geräte-TUNID in Ordnung ist.
Access error	Das verwendete Kennwort berechtigt nicht zum Ändern von Konfigurationen. Prüfen Sie, ob das richtige Kennwort verwendet wird.
The device cannot be accessed or the device type or password is different.	1. Das Gerät wurde gerade zurückgesetzt, oder die Spannungsversorgung wurde aus- und wieder eingeschaltet, und das Gerät ist nicht kommunikationsbereit (d.h. nicht online, Kontrolleuchte „NS“ blinkt oder leuchtet grün). Vergewissern Sie sich, dass das Gerät kommunikationsbereit ist, und führen Sie dann die Rücksetzung durch.
	2. Das für die Rücksetzung angegebene Gerät unterstützt diesen Dienst möglicherweise nicht. Prüfen Sie, ob die Knotenadresse des Geräts stimmt.
	3. Die Konfigurationsdaten sind gesperrt (Kontrollleuchte LOCK leuchtet). Heben Sie die Sperre auf, und führen Sie die gewünschte Rücksetzung durch.
	4. Das Gerät führt eine Sicherheits-E/A-Kommunikation durch und kann die gewünschte Rücksetzung daher nicht durchführen. Ändern Sie den Betriebsmodus des betreffenden Sicherheits-Masters zu IDLE. Führen Sie dann die gewünschte Rücksetzung durch.
Connection failed.	Verbindungsfehler beim Versuch, ein Gerät im DeviceNet Netzwerk über die USB-Schnittstelle des Sicherheitsnetzwerk-Controllers NE1A zurückzusetzen. Vergewissern Sie sich, dass die Spannungsversorgung des Geräts eingeschaltet ist, und führen Sie die Rücksetzung erneut durch. Möglicherweise wurde die Kommunikation auch durch einen hohen Störpegel oder andere Faktoren beeinträchtigt. Prüfen Sie die folgenden Punkte. • Haben alle Knoten dieselbe Baudrate? • Stimmen die Kabellängen (Sammel- und Abzweigleitungen)? • Ist das Kabel unterbrochen oder lose? • Sind die beiden Enden (und nur diese) des Netzwerkstrangs durch Abschlusswiderstände terminiert? • Gibt es einen hohen Störpegel?

10-7 Fehler beim Wechsel des Betriebsmodus

10-7-1 Übersicht

Der Sicherheitsnetzwerk-Controller NE1A kann bei einem Wechsel des Betriebsmodus Fehlermeldungen generieren. Anhand der vom Netzwerkkonfigurator angezeigten Meldungen kann die Fehlerursache identifiziert und der Fehler behoben werden.

10-7-2 Fehlermeldungen und Abhilfemaßnahmen

Meldung des Netzwerkkonfigurators	Abhilfemaßnahmen
Cannot be executed in the current mode.	1. Das Gerät wurde nicht konfiguriert (Konfigurationsmodus). Laden Sie die Geräteparameter herunter.
	2. Es ist ein kritischer Fehler (Abbruchfehler) aufgetreten. Stellen Sie die Schalter korrekt ein, oder führen Sie eine Rücksetzung durch, um die Konfigurationsdaten zu löschen. Laden Sie die Geräteparameter nach dem Löschen der Konfigurationsdaten erneut herunter.
Already set to the specified mode.	Der Sicherheitsnetzwerk-Controller NE1A-SCPU01 befindet sich bereits im angegebenen Betriebsmodus.
The device has a different TUNID.	Die im Sicherheitsnetzwerk-Controller NE1A gespeicherte TUNID entspricht nicht der im Netzwerkkonfigurator festgelegten TUNID. Prüfen Sie, ob die Knotenadresse des Geräts übereinstimmt. Falls ja, bedeutet dies, dass die Netzwerknummer des Geräts nicht mit der Netzwerknummer des Netzwerkkonfigurators übereinstimmt. Wählen Sie im Netzwerkkonfigurator ***Network – Upload***, um die Netzwerknummern anzugleichen.
Access error	Das verwendete Kennwort berechtigt nicht zum Ändern des Betriebsmodus. Prüfen Sie, ob das richtige Kennwort verwendet wird.
The device cannot be accessed or the device type or password is different.	1. Das Gerät wurde gerade zurückgesetzt, oder die Spannungsversorgung wurde aus- und wieder eingeschaltet, und das Gerät ist nicht kommunikationsbereit (d.h. nicht online, Kontrolleuchte „NS“ blinkt oder leuchtet grün). Vergewissern Sie sich, dass das Gerät kommunikationsbereit ist, und führen Sie dann die Rücksetzung durch.
	2. Das Gerät, dessen Betriebsmodus geändert werden sollte, unterstützt diesen Dienst möglicherweise nicht. Prüfen Sie, ob die Knotenadresse des Geräts stimmt.
Connection failed.	Verbindungsfehler beim Versuch, den Betriebsmodus eines Geräts im DeviceNet Netzwerk über die USB-Schnittstelle des Sicherheitsnetzwerk-Controllers NE1A zu ändern. Vergewissern Sie sich, dass die Spannungsversorgung des Geräts eingeschaltet ist, und führen Sie die Rücksetzung erneut durch. Möglicherweise wurde die Kommunikation auch durch einen hohen Störpegel oder andere Faktoren beeinträchtigt. Prüfen Sie die folgenden Punkte. • Haben alle Knoten dieselbe Baudrate? • Stimmen die Kabellängen (Sammel- und Abzweigleitungen)? • Ist das Kabel unterbrochen oder lose? • Sind die beiden Enden (und nur diese) des Netzwerkstrangs durch Abschlusswiderstände terminiert? • Gibt es einen hohen Störpegel?

10-8 Verbindungsstatus-Tabellen

10-8-1 Übersicht

Bei Fehlern während des Verbindungsaufbaus zwischen dem Sicherheitsnetzwerk-Controller NE1A und einem DST1 Sicherheits-E/A-Modul oder einem als Slave konfigurierten Sicherheitsnetzwerk-Controller NE1A zeigt die Siebensegmentanzeige den Fehlercode „d6“ oder „d5“ an.

Überprüfen Sie den auf der Registerkarte „Safety Connection“ im Fenster „Monitor Device“ angezeigten Statuscode (Fehlercode), und ergreifen Sie die entsprechende Abhilfemaßnahme.

10-8-2 Verbindungsstatus für DST1

Status		Abhilfemaßnahme
00:0001	Normal communications	Die Status der Sicherheits-E/A-Verbindung ist normal.
01:0001	Safety I/O Connection Timeout	Zeitüberschreitung der Sicherheits-E/A-Verbindung. Prüfen Sie die folgenden Punkte. • Haben alle Knoten dieselbe Baudrate? • Stimmen die Kabellängen (Sammel- und Abzweigleitungen)? • Ist das Kabel unterbrochen oder lose? • Sind die beiden Enden (und nur diese) des Netzwerkstrangs durch Abschlusswiderstände terminiert? • Gibt es einen hohen Störpegel? • Ist die zugeordnete Netzwerkbandbreite geeignet?
01:0105	Configuration Owner Error	Der Sicherheits-Slave wurde beim letzten Mal über ein Konfigurations-Tool oder einen Sicherheits-Master unter einer anderen Knotenadresse konfiguriert. Setzen Sie den Sicherheits-Slave auf die Standardeinstellungen zurück. Laden Sie die Parameter dann erneut herunter. Informationen zu Konfigurationseignern finden Sie unter *5-1-2 Festlegen der Einstellungen für Sicherheitsverbindungen* im Konfigurationshandbuch *DeviceNet Safety System (Z905)*.
01:0106	Output connection Owner Error	Der Sicherheits-Slave hat beim letzten Mal Sicherheits-E/A-Verbindungen mit einem Sicherheits-Master unter einer anderen Knotenadresse hergestellt. Setzen Sie den Sicherheits-Slave auf die Standardeinstellungen zurück. Laden Sie die Parameter dann erneut herunter. Informationen zu Eignern von Ausgangsverbindungen finden Sie unter *5-1-2 Festlegen der Einstellungen für Sicherheitsverbindungen* im Konfigurationshandbuch *DeviceNet Safety System (Z905)*.
01:0110	Device Not Configurated	Der Sicherheits-Slave wurde nicht konfiguriert. Laden Sie die Geräteparameter in den Sicherheits-Slave.
01:0113	No. of Connections Error	Die eingestellte Anzahl von Sicherheits-E/A-Verbindungen überschreitet die vom Sicherheits-Slave unterstütze Obergrenze. Korrigieren Sie die Einstellung „Safety Connection“ des jeweiligen Sicherheits-Masters.
01:0114	Vendor ID or Program Code Error	Die Gerätedaten (Vendor-ID oder Produktcode) im Konfigurator stimmen nicht mit dem tatsächlich verwendeten Gerät überein. • Prüfen Sie den Sicherheits-Slave mit (***Device – Parameter – Verify***) darauf, ob das Gerät im System mit dem im Sicherheits-Master registrierten Gerät übereinstimmt. • Falls sie übereinstimmen, löschen Sie zunächst die im Sicherheits-Master registrierten Verbindungen und registrieren Sie dann erneut.
01:0115	Device Type Error	Die Gerätedaten (Gerätetyp) im Konfigurator stimmen nicht mit dem tatsächlich verwendeten Gerät überein. • Prüfen Sie den Sicherheits-Slave mit (***Device – Parameter – Verify***) darauf, ob das Gerät im System mit dem im Sicherheits-Master registrierten Gerät übereinstimmt. • Falls sie übereinstimmen, löschen Sie zunächst die im Sicherheits-Master registrierten Verbindungen und registrieren Sie dann erneut.
01:0116	Revision Error	Die Gerätedaten (Revision) im Konfigurator stimmen nicht mit dem tatsächlich verwendeten Gerät überein. • Prüfen Sie den Sicherheits-Slave mit (***Device – Parameter – Verify***) darauf, ob das Gerät im System mit dem im Sicherheits-Master registrierten Gerät übereinstimmt. • Falls sie übereinstimmen, löschen Sie zunächst die im Sicherheits-Master registrierten Verbindungen und registrieren Sie dann erneut.

Status		Abhilfemaßnahme
01:0117	Connection Path Error	1. Für den Sicherheits-Slave wurden mehrere Sicherheits-E/A-Verbindungen konfiguriert. • Ändern Sie die Einstellung „Safety Connection“ für den Sicherheits-Master dahingehend, dass es nur eine Verbindung gibt. Setzen Sie dann den Sicherheits-Slave auf die Standardeinstellungen zurück, und laden Sie die Parameter erneut in den Sicherheits-Slave. 2. Dieselbe Ausgangsbaugruppe eines Sicherheits-Slaves wurde für einen Sicherheits-Master und einen Standard-Master verwendet. • Während die Nummern für Eingangsbaugruppen vervielfältigt werden können, ist dies bei Ausgangsbaugruppen nicht möglich. Überprüfen Sie die Einstellung „Safety Connection“ für den Sicherheits-Master und den Standard-Master. Stellen Sie dann die Standardeinstellungen für den Sicherheits-Slave wieder her, und laden Sie die Geräteparameter wieder in den Sicherheits-Slave. • Bleibt der Fehler auch nach der obigen Abhilfemaßnahme bestehen, löschen Sie die im Sicherheits-Master registrierten Verbindungen und registrieren Sie sie dann erneut.
01:031E	No. of Connections Error	Die eingestellte Anzahl von Sicherheits-E/A-Verbindungen überschreitet die vom Sicherheits-Slave unterstütze Obergrenze. Korrigieren Sie die Einstellung „Safety Connection“ des jeweiligen Sicherheits-Masters. Vergewissern Sie sich insbesondere, dass pro Multicast-Verbindung nicht mehr als 15 Sicherheits-Masters konfiguriert sind; insgesamt dürfen es nicht mehr als 30 sein.
01:031F	Connection ID Resource Error	Die maximale Anzahl von Verbindungs-IDs für einen Sicherheits-Master (12) wurde überschritten. Ändern Sie die ID-Zuordnung unter ***Edit Safety Connection – Expansion Connection Setting*** zu „Check Produced IDs in the Safety Slave“ in der entsprechenden Sicherheits-E/A-Verbindungseinstellung („Safety Input Assembly“), und laden Sie dann die Geräteparameter erneut in den Sicherheits-Master.
01:07FF	Non-existent Safety Slave	Der Sicherheits-Slave wurde dem Netzwerk möglicherweise nicht ordnungsgemäß hinzugefügt. Vergewissern Sie sich, dass der entsprechende „Sicherheits-Slave“ online ist (d.h. Kontrollleuchte „NS“ blinkt oder leuchtet grün). Wenn der Sicherheits-Slave nicht online ist, prüfen Sie die folgenden Punkte: • Stimmt die Knotenadresse für den Sicherheits-Slave? • Haben alle Knoten dieselbe Baudrate? • Stimmen die Kabellängen (Sammel- und Abzweigleitungen)? • Ist das Kabel unterbrochen oder lose? • Sind die beiden Enden (und nur diese) des Netzwerkstrangs durch Abschlusswiderstände terminiert? • Gibt es einen hohen Störpegel?
01:080C	Safety Signature Mismatch	Die vom Sicherheits-Master überwachte Sicherheitssignatur für den Sicherheits-Slave stimmt nicht mit der tatsächlichen Sicherheitssignatur des Sicherheits-Slaves überein. • Setzen Sie den Sicherheits-Slave auf die Standardeinstellungen zurück. Laden Sie die Parameter dann erneut herunter. • Wenn die obige Abhilfemaßnahme nicht funktioniert, löschen Sie die im Sicherheits-Master registrierten Verbindungen und registrieren Sie sie dann erneut.
01:080E	TUNID Mismatch	Die vom Sicherheits-Master überwachte TUNID für den Sicherheits-Slave stimmt nicht mit der tatsächlichen TUNID des Sicherheits-Slaves überein. • Setzen Sie den Sicherheits-Slave auf die Standardeinstellungen zurück. Laden Sie dann die richtigen Geräteparameter herunter. • Wenn die obige Abhilfemaßnahme nicht funktioniert, löschen Sie die im Sicherheits-Master registrierten Verbindungen und registrieren Sie sie dann erneut. Informationen zu TUNIDs finden Sie unter *3-4-2 Netzwerknummern* im Konfigurationshandbuch *DeviceNet Safety System* (Z905).
01:080F	Safety Configuration not possible	Die Konfiguration für den Sicherheits-Slave ist gesperrt, und *Configure the target device* ist als Einstellung „Open Type“ für die Verbindung des Sicherheits-Masters ausgewählt. • Heben Sie die Konfigurationssperre für den Sicherheits-Slave auf, um ihn über den Sicherheits-Master zu konfigurieren. • Um den Sicherheits-Slave über ein Konfigurations-Tol zu konfigurieren, setzen Sie die Verbindung des Sicherheits-Masters unter „Open Type“ auf *Check the safety signature* . Setzen Sie dann den Sicherheits-Slave auf die Standardeinstellungen zurück, und laden Sie die Parameter erneut in den Sicherheits-Slave.

10-8-3 Verbindungsstatus für den Sicherheitsnetzwerk-Controller NE1A (Sicherheits-Slave-Funktion)

Status		Abhilfemaßnahmen
00:0001	Normal communications	Die Status der Sicherheits-E/A-Verbindung ist normal.
01:0001	Safety I/O Connection Timeout	Zeitüberschreitung der Sicherheits-E/A-Verbindung. Prüfen Sie die folgenden Punkte. • Haben alle Knoten dieselbe Baudrate? • Stimmen die Kabellängen (Sammel- und Abzweigleitungen)? • Ist das Kabel unterbrochen oder lose? • Sind die beiden Enden (und nur diese) des Netzwerkstrangs durch Abschlusswiderstände terminiert? • Gibt es einen hohen Störpegel? • Ist die zugeordnete Netzwerkbandbreite geeignet?
01:0106	Output Connection Owner Error	Der Sicherheits-Slave hat zuvor eine Sicherheits-E/A-Verbindung mit einem Sicherheits-Master unter einer anderen Knotenadresse hergestellt. Setzen Sie den Sicherheits-Slave auf die Standardeinstellungen zurück. Laden Sie die Parameter dann erneut herunter. Informationen zu Eignern von Ausgangsverbindungen finden Sie unter *5-1-2 Festlegen der Einstellungen für Sicherheitsverbindungen* im Konfigurationshandbuch *DeviceNet Safety System (Z905)*.
01:0109	Data Size Error	Die eingestellte E/A-Größe für den Sicherheits-Slave NE1A stimmt nicht mit der für die Verbindung des Sicherheits-Masters eingestellten Größe überein. Die E/A-Einstellung des Sicherheits-Slaves wurde möglicherweise verändert. Löschen Sie daher die im Sicherheits-Master registrierten Verbindungen und registrieren Sie sie dann erneut.
01:0110	Unconfigured Device	Der Sicherheits-Slave wurde nicht konfiguriert. Laden Sie die Geräteparameter in den Sicherheits-Slave.
01:0111	EPI Error	Das für die Verbindung des Sicherheits-Masters eingestellte EPI ist kürzer als die Zykluszeit des Sicherheits-Slaves. Das EPI muss länger sein als die Zykluszeiten von Sicherheits-Master und Sicherheits-Slave. Prüfen Sie die Einstellung der Sicherheits-E/A-Verbindungen im Sicherheits-Master.
01:0113	No. of Connections Error	Die eingestellte Anzahl von Sicherheits-E/A-Verbindungen überschreitet die vom Sicherheits-Slave unterstütze Obergrenze. Prüfen Sie die Einstellung der Sicherheits-E/A-Verbindungen im jeweiligen Sicherheits-Master.
01:0114	Vendor ID or Product Code Error	Die Gerätedaten (Vendor-ID oder Produktcode) im Konfigurator stimmen nicht mit dem tatsächlich verwendeten Gerät überein. • Prüfen Sie den Sicherheits-Slave mit (***Device – Parameter – Verify***) darauf, ob das Gerät im System mit dem im Sicherheits-Master registrierten Gerät übereinstimmt. • Falls sie übereinstimmen, löschen Sie zunächst die im Sicherheits-Master registrierten Verbindungen und registrieren Sie dann erneut.
01:0115	Device Type Error	Die Gerätedaten (Gerätetyp) im Konfigurator stimmen nicht mit dem tatsächlich verwendeten Gerät überein. • Prüfen Sie den Sicherheits-Slave mit (***Device – Parameter – Verify***) darauf, ob das Gerät im System mit dem im Sicherheits-Master registrierten Gerät übereinstimmt. • Falls sie übereinstimmen, löschen Sie zunächst die im Sicherheits-Master registrierten Verbindungen und registrieren Sie dann erneut.
01:0116	Firmware Revision Error	Die Gerätedaten (Firmware-Revision) im Konfigurator stimmen nicht mit dem tatsächlich verwendeten Gerät überein. • Prüfen Sie den Sicherheits-Slave mit (***Device – Parameter – Verify***) darauf, ob das Gerät im System mit dem im Sicherheits-Master registrierten Gerät übereinstimmt. • Falls sie übereinstimmen, löschen Sie zunächst die im Sicherheits-Master registrierten Verbindungen und registrieren Sie dann erneut.

Status		Abhilfemaßnahmen
01:0117	Connection Path Error	Für einen Sicherheits-Slave-E/A wurden mehrere Singlecast-Sicherheits-E/A-Verbindungen oder eine Multicast-Sicherheits-E/A-Verbindung mit abweichendem EPI konfiguriert. • Um einen Sicherheits-Slave-E/A für mehrere Sicherheits-Master nutzen zu können, müssen Sie alle EPIs vereinheitlichen und als Verbindungsart „Multicast“ angeben. • NE1A Sicherheits-Slaves können nicht mehrere Singlecast-Sicherheits-E/A-Verbindungen je Sicherheits-Slave-E/A unterstützen. Konfigurieren Sie mehrere Verbindungspfade für die E/A des Sicherheits-Slaves. • Wenn die Verbindung mit der obigen Abhilfemaßnahme nicht wiederhergestellt wird, löschen Sie die im Sicherheits-Master registrierten Verbindungen und registrieren Sie sie dann erneut.
01:031E	No. of Connections Error	Die eingestellte Anzahl von Sicherheits-E/A-Verbindungen überschreitet die vom Sicherheits-Slave unterstütze Obergrenze. Korrigieren Sie die Einstellung „Safety Connection“ des jeweiligen Sicherheits-Masters. Vergewissern Sie sich insbesondere, dass pro Multicast-Verbindung nicht mehr als 15 Sicherheits-Master konfiguriert sind; insgesamt dürfen es nicht mehr als 60 sein.
01:031F	Connection ID Resource Error	Die maximale Anzahl von Verbindungs-IDs für einen Sicherheits-Master (12) wurde überschritten. Ändern Sie die ID-Zuordnung unter ***Edit Safety Connection – Expansion Connection Setting*** zu „Check Produced IDs in the Safety Slave“ in der entsprechenden Sicherheits-E/A-Verbindungseinstellung („Safety Input Assembly“), und laden Sie dann die Geräteparameter erneut in den Sicherheits-Master.
01:07FF	Non-existent Safety Slave	Der Sicherheits-Slave wurde dem Netzwerk möglicherweise nicht ordnungsgemäß hinzugefügt. Vergewissern Sie sich, dass der entsprechende „Sicherheits-Slave“ online ist (d.h. Kontrollleuchte „NS“ blinkt oder leuchtet grün). Wenn der Sicherheits-Slave nicht online ist, prüfen Sie die folgenden Punkte: • Stimmt die Knotenadresse für den Sicherheits-Slave? • Haben alle Knoten dieselbe Baudrate? • Stimmen die Kabellängen (Sammel- und Abzweigleitungen)? • Ist das Kabel unterbrochen oder lose? • Sind die beiden Enden (und nur diese) des Netzwerkstrangs durch Abschlusswiderstände terminiert? • Gibt es einen hohen Störpegel?
01:080C	Safety Signature Mismatch	Die vom Sicherheits-Master überwachte Sicherheitssignatur für den Sicherheits-Slave stimmt nicht mit der tatsächlichen Sicherheitssignatur des Sicherheits-Slaves überein. • Setzen Sie den Sicherheits-Slave auf die Standardeinstellungen zurück. Laden Sie die Parameter dann erneut herunter. • Wenn die obige Abhilfemaßnahme nicht funktioniert, löschen Sie die im Sicherheits-Master registrierten Verbindungen und registrieren Sie sie dann erneut.
01:080E	TUNID Mismatch	Die vom Sicherheits-Master überwachte TUNID für den Sicherheits-Slave stimmt nicht mit der tatsächlichen TUNID des Sicherheits-Slaves überein. • Setzen Sie den Sicherheits-Slave auf die Standardeinstellungen zurück. Laden Sie dann die richtigen Geräteparameter herunter. • Wenn die obige Abhilfemaßnahme nicht funktioniert, löschen Sie die im Sicherheits-Master registrierten Verbindungen und registrieren Sie sie dann erneut. Informationen zu TUNIDs finden Sie unter *3-4-2 Netzwerknummern* im Konfigurationshandbuch *DeviceNet Safety System* (Z905).
D0:0001	IDLE (Leerlauf)	Der Sicherheits-Master NE1A befindet sich im Modus IDLE, folglich wurden keine Sicherheits-E/A-Verbindungen hergestellt. Ändern Sie den Betriebsmodus des Sicherheits-Masters NE1A zu RUN.

ABSCHNITT 11
Wartung und Inspektion

11-1 Inspektion 224
11-2 Austausch des Sicherheitsnetzwerk-Controllers NE1A 225

11-1 Inspektion

Zur Sicherstellung der einwandfreien Funktion des Sicherheitsnetzwerk-Controllers NE1A ist eine tägliche oder regelmäßige Inspektion erforderlich.

- Kontrollieren Sie, dass der Sicherheitsnetzwerk-Controller NE1A im Rahmen seiner Spezifikationen eingesetzt wird.
- Kontrollieren Sie die Zulässigkeit der Installationsbedingungen und der Verdrahtung des Sicherheitsnetzwerk-Controllers NE1A.
- Führen Sie eine Diagnose der Sicherheitsfunktionen durch, um deren Zuverlässigkeit im Betrieb sicherzustellen.

11-2 Austausch des Sicherheitsnetzwerk-Controllers NE1A

Beachten Sie bei einem eventuell erforderlichen Austausch des Sicherheitsnetzwerk-Controllers NE1A die folgenden Punkte:

- Nehmen Sie den Sicherheitsnetzwerk-Controller NE1A nicht auseinander, und versuchen Sie nicht, ihn zu reparieren oder zu modifizieren, da sonst die Gefahr einer Beeinträchtigung oder eines Ausfalls der ursprünglichen Sicherheitsfunktionen besteht.
- Stellen Sie sicher, dass der Austausch des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 unter sicheren Bedingungen erfolgt.
- Um elektrische Schläge oder eine unerwartete Aktivierung von Geräten zu verhindern, muss die Spannungsversorgung vor dem Austausch des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 ausgeschaltet werden.
- Überprüfen Sie nach dem Austausch die neuen Baugruppe auf fehlerfreie Funktion.
- Wenn Sie die defekte Baugruppe zur Reparatur einsenden, legen Sie eine Notiz bei, die möglichst viele Angaben über den Fehler enthält. Senden Sie die defekte Baugruppe an den Omron Vertrieb. Adressen und Telefonnummern finden Sie auf der Rückseite dieses Bedienerhandbuchs.

⚠ VORSICHT

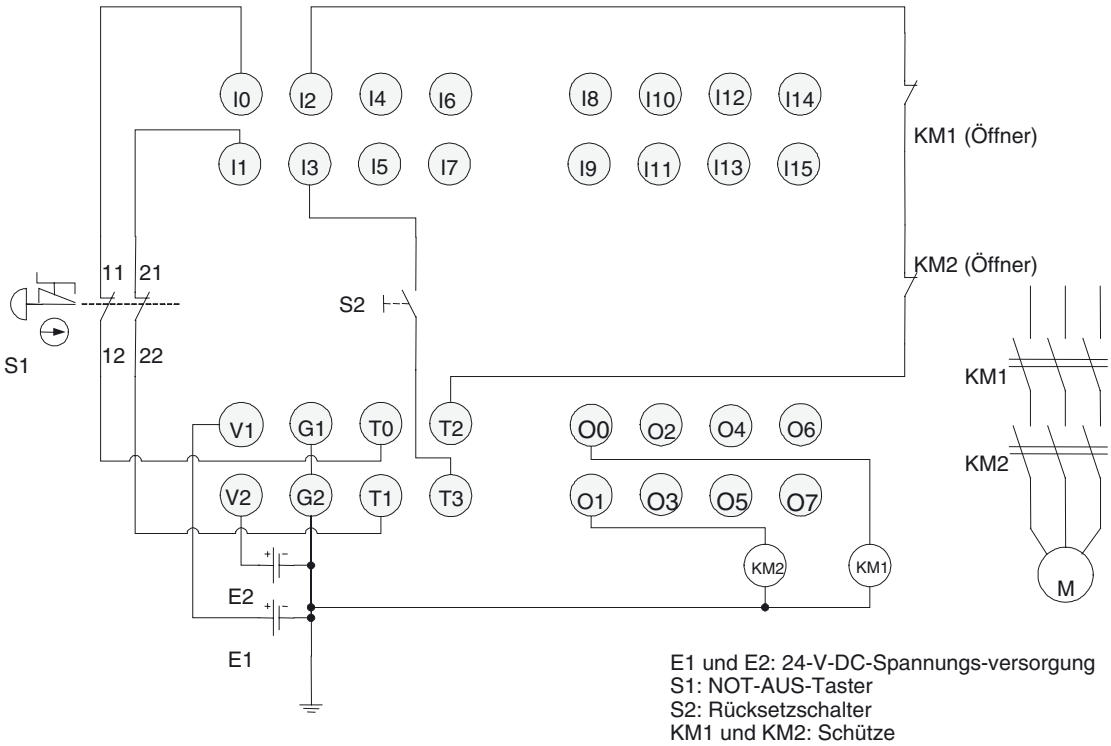
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, müssen vor der Wiederaufnahme des Betriebs nach einem Austausch des Sicherheitsnetzwerk-Controllers NE1A alle erforderlichen Konfigurationsinformationen (z. B. Anwenderprogramm) neu gesetzt werden. Prüfen Sie vor der eigentlichen Inbetriebnahme die ordnungsgemäße Funktion der Sicherheitsfunktionen.

Anhang A

Anhang 1: Anwendungs- und Konfigurationsbeispiele

A-1-1 NOT-AUS-Anwendung: Zweikanal-Modus mit manueller Rücksetzung

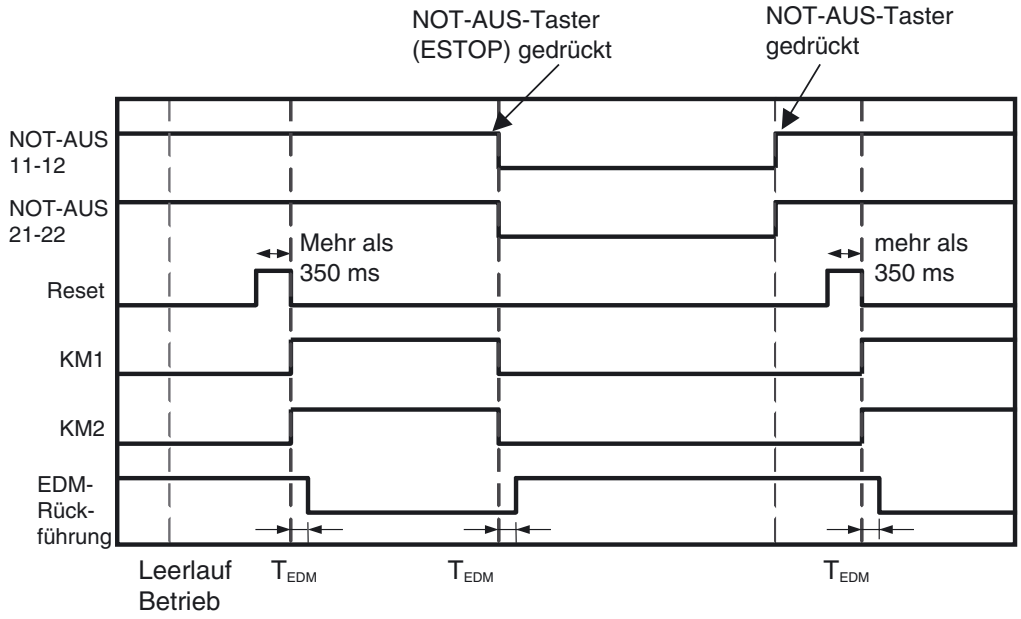
Verdrahtungsdiagramm



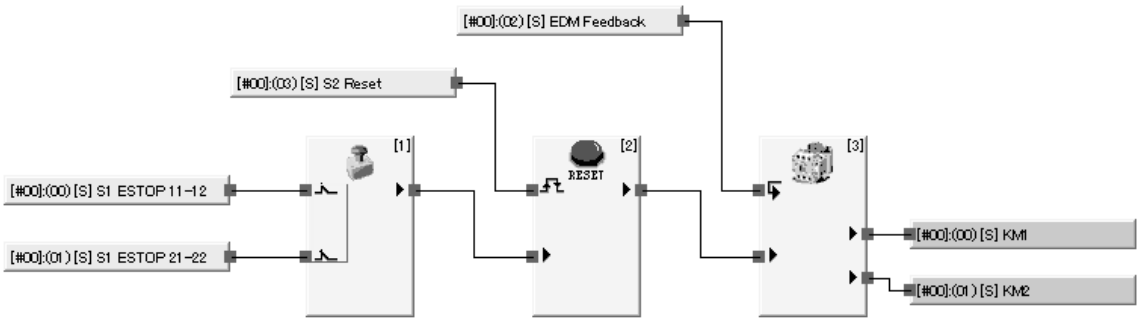
Hinweis (1) Schließen Sie die Klemmen V0 und G0 (Spannungsversorgung für interne Schaltkreise) an eine 24-V-DC-Spannungsversorgung an.

(2) Das Beispiel zeigt die Klemmenbelegung des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 (-V1).

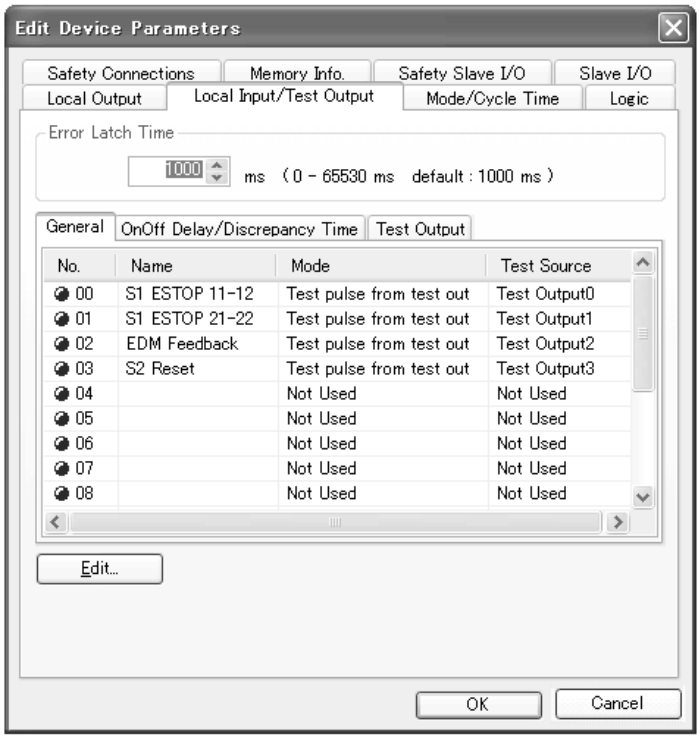
Zeitablaufdiagramm



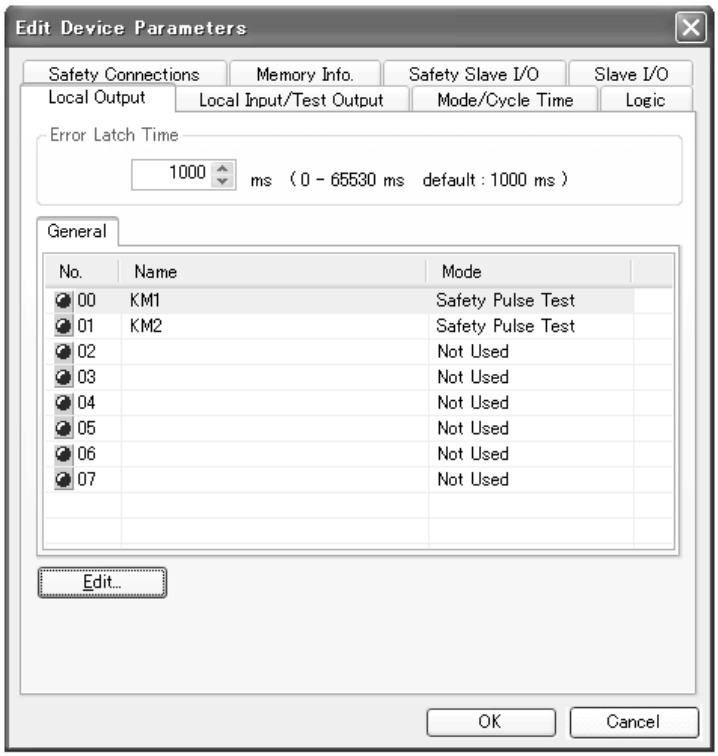
Programmierbeispiel



Lokale Eingänge / Testausgänge

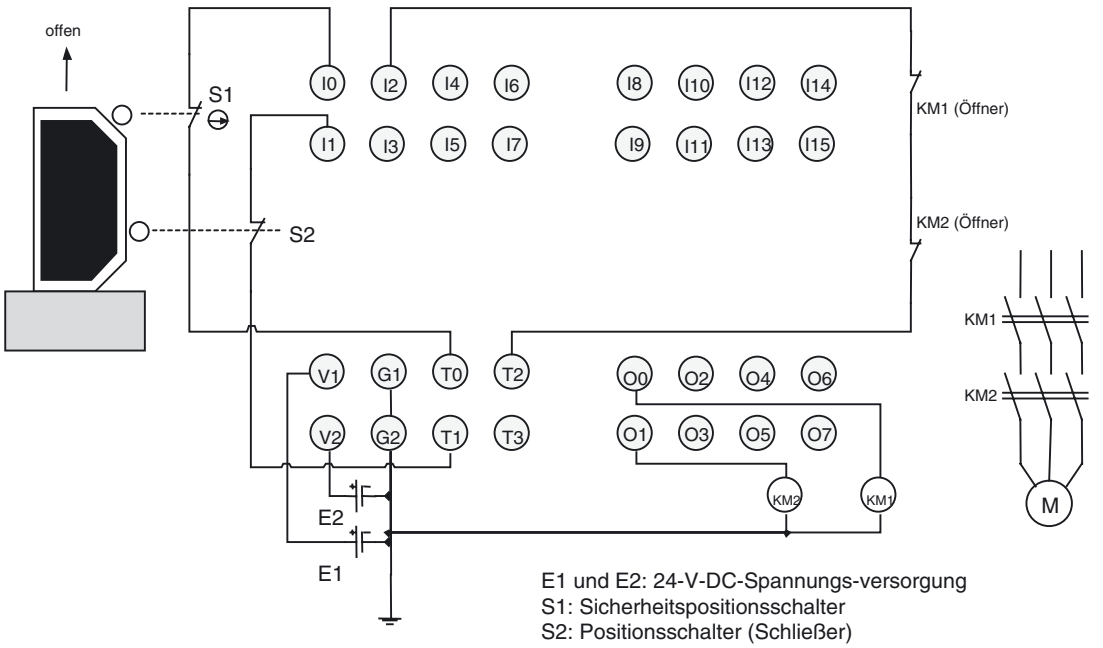


Lokale Ausgänge



A-1-2 Sicherheitstür-Überwachung: Zweikanal-Positionsschalter mit automatischer Rücksetzung

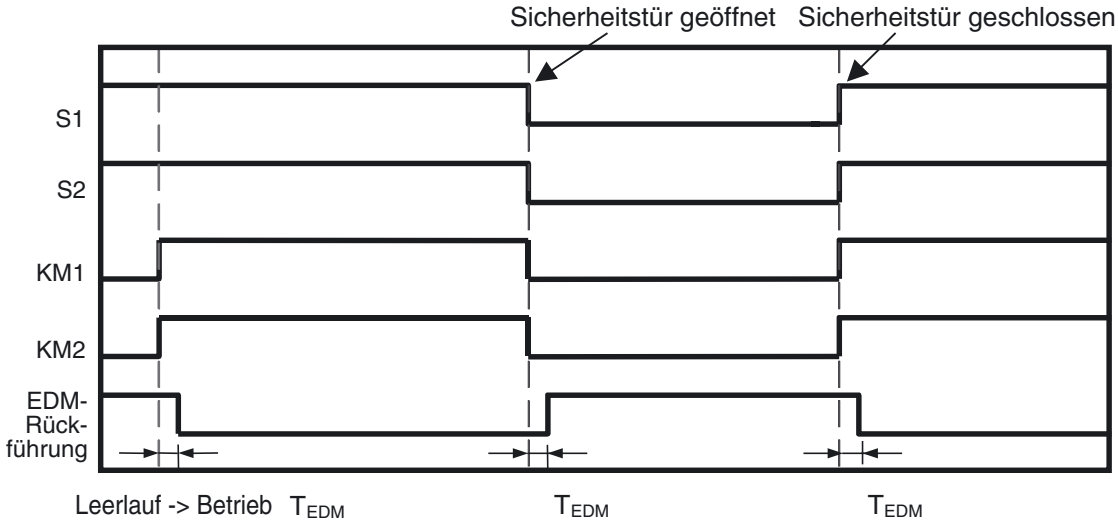
Verdrahtungsbeispiel



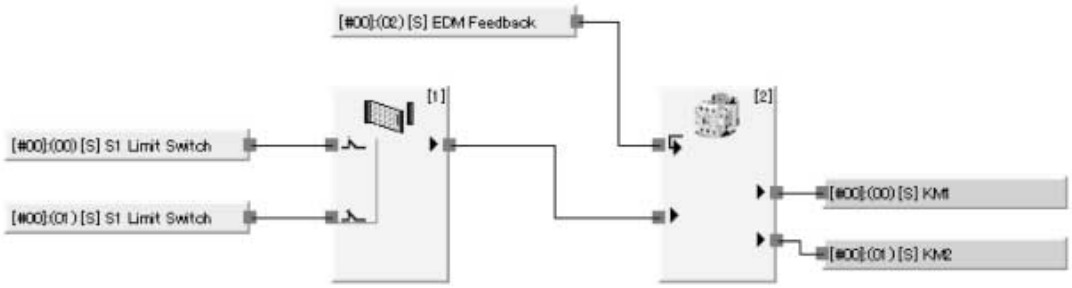
Hinweis (1) Schließen Sie die Klemmen V0 und G0 (Spannungsversorgung für interne Schaltkreise) an eine 24-V-DC-Spannungsversorgung an.

(2) Das Beispiel zeigt die Klemmenbelegung des Sicherheitsnetzwerk-Controllers NE1A-SCPU01(-V1).

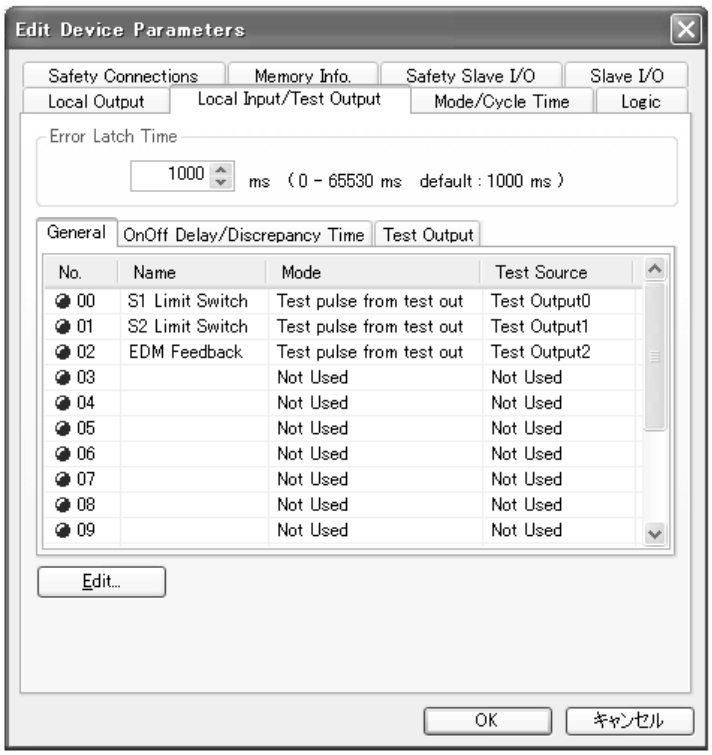
Zeitablaufdiagramm



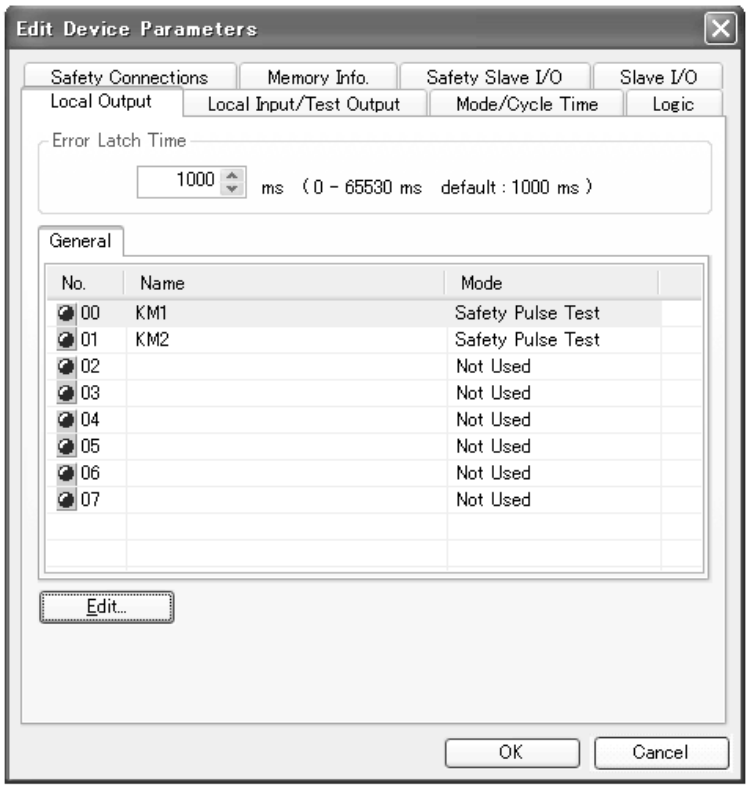
Programmierbeispiel



Lokale Eingänge / Testausgänge

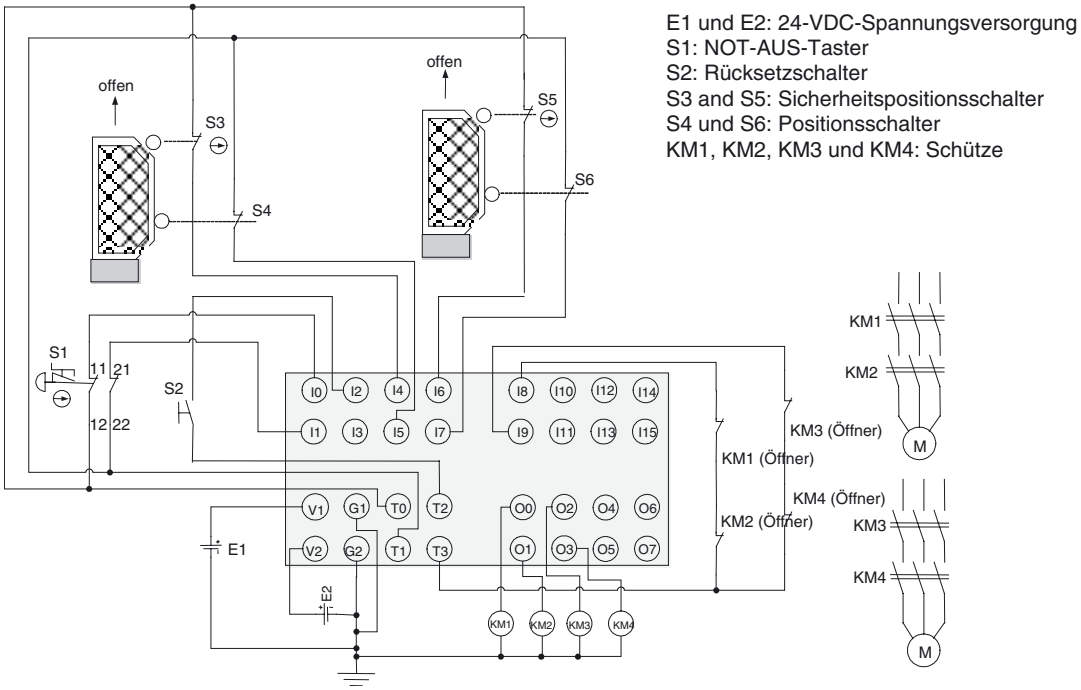


Lokale Ausgänge



A-1-3 Sicherheitstür-Überwachung: Zweikanal-Türschalter mit automatischer Rücksetzung und Zweikanal-NOT-AUS-Taster mit manueller Rücksetzung

Verdrahtungsbeispiel

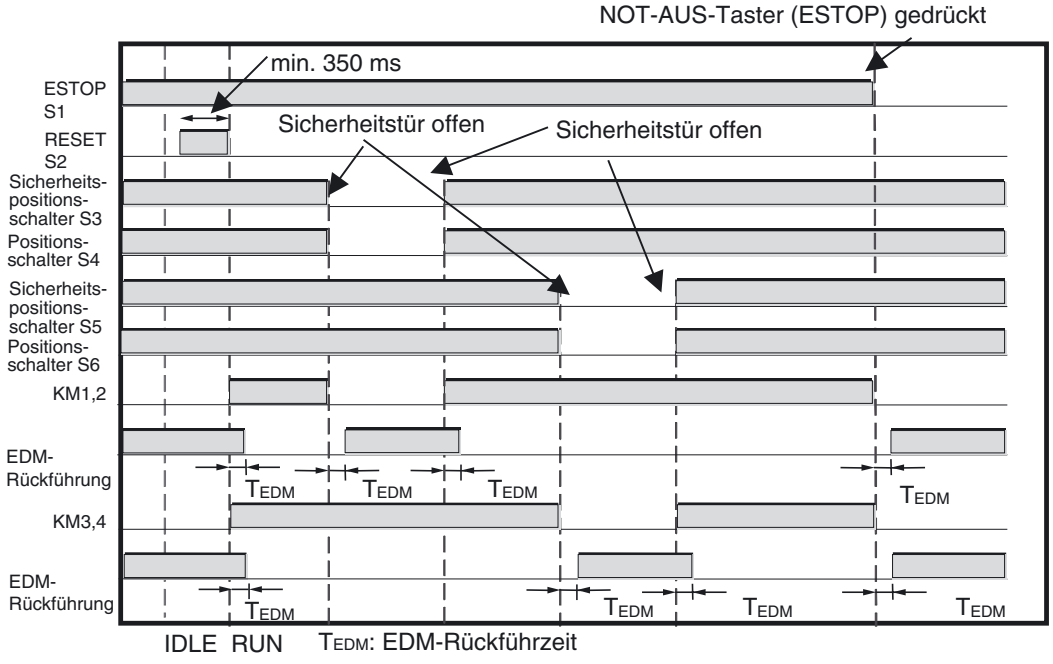


E1 und E2: 24-VDC-Spannungsversorgung
S1: NOT-AUS-Taster
S2: Rücksetzschalter
S3 and S5: Sicherheitspositionsschalter
S4 und S6: Positionsschalter
KM1, KM2, KM3 und KM4: Schütze

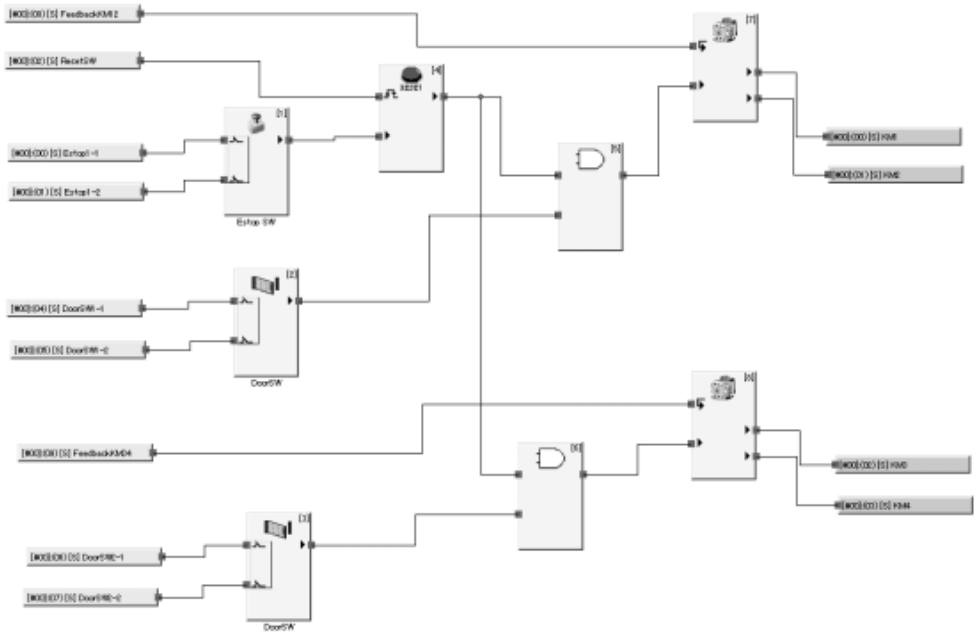
Hinweis (1) Schließen Sie die Klemmen V0 und G0 (Spannungsversorgung für interne Schaltkreise) an eine 24-V-DC-Spannungsversorgung an.

(2) Das Beispiel zeigt die Klemmenbelegung des Sicherheitsnetzwerk-Controllers NE1A-SCPU01(-V1).

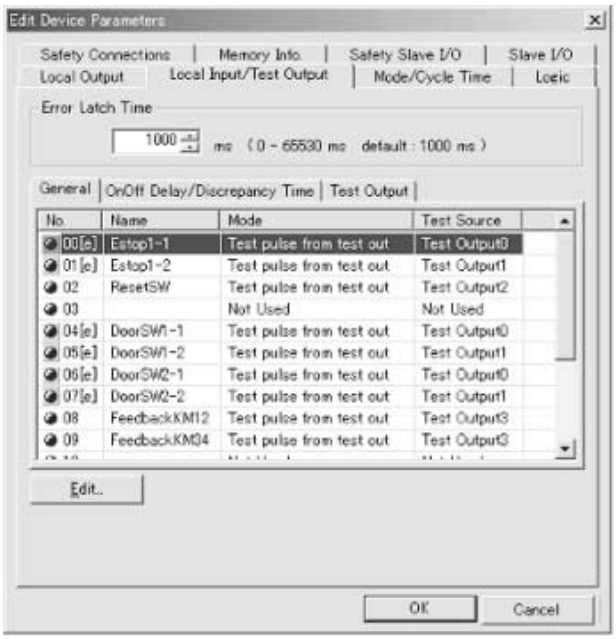
Zeitablaufdiagramm



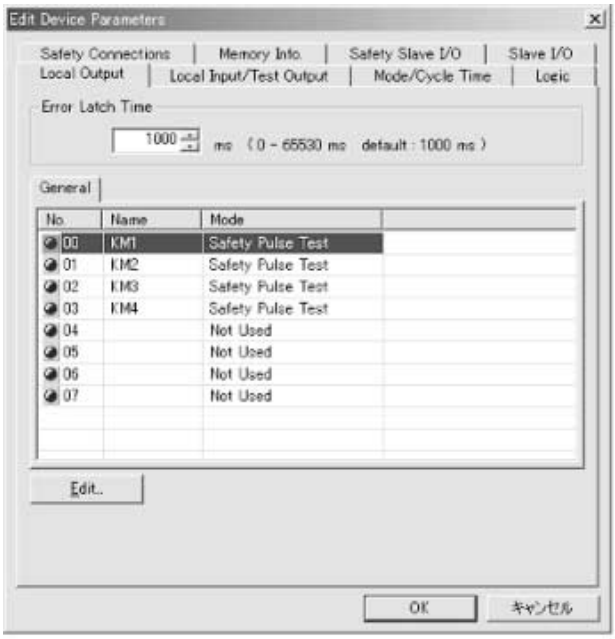
Programmierbeispiel



Lokale Eingänge / Testausgänge

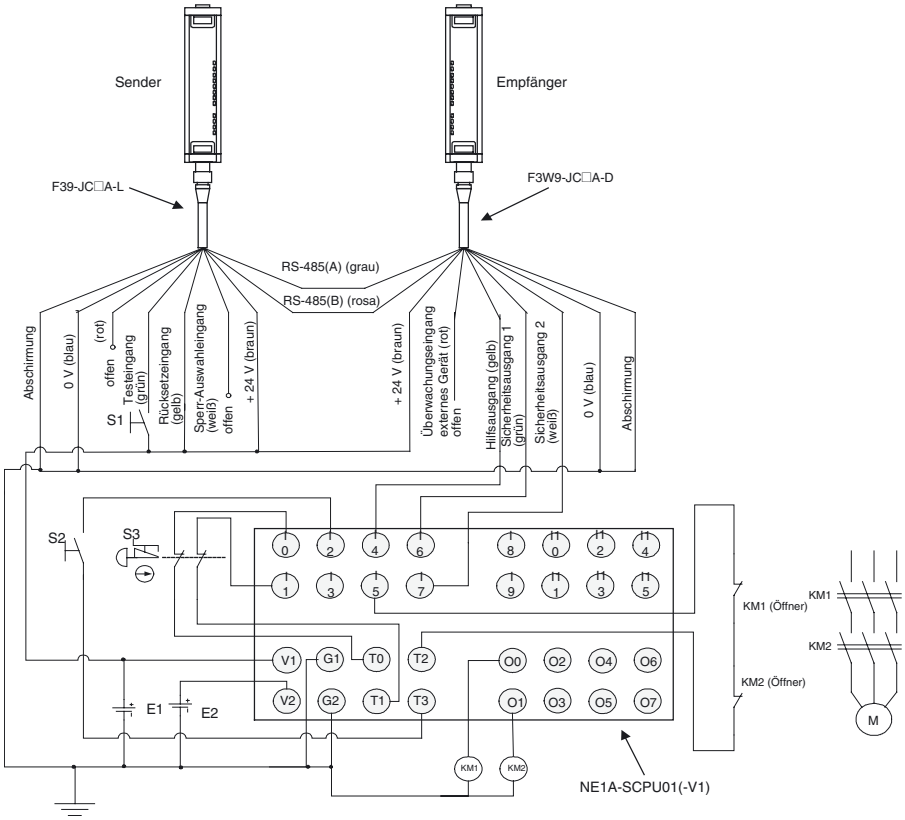

Edit Device Parameters
Safety Connections
Memory Info.
Safety Slave I/O
Slave I/O
Local Output
Local Input/Test Output
Mode/Cycle Time
Logic
Error Latch Time
1000
ms (0 - 65530 ms default : 1000 ms)
General
OnOff Delay/Discrepancy Time
Test Output
No.
Name
Mode
Test Source
00[e] Estop1-1 Test pulse from test out Test Output0
01[e] Estop1-2 Test pulse from test out Test Output1
02 ResetSW Test pulse from test out Test Output2
03 Not Used Not Used
04[e] DoorSW1-1 Test pulse from test out Test Output0
05[e] DoorSW1-2 Test pulse from test out Test Output1
06[e] DoorSW2-1 Test pulse from test out Test Output0
07[e] DoorSW2-2 Test pulse from test out Test Output1
08 FeedbackKM12 Test pulse from test out Test Output3
09 FeedbackKM34 Test pulse from test out Test Output3
Edit...
OK
Cancel

Lokale Ausgänge



A-1-4 Sicherheitslichtgitter: Zweikanal-Sicherheitslichtgitter mit manueller Rücksetzung und Zweikanal-NOT-AUS-Taster mit manueller Rücksetzung

Verdrahtungsbeispiel



E1 und E2: 24-VDC-Spannungsversorgung
S1: Rücksetztaster
S2: Rücksetztaster

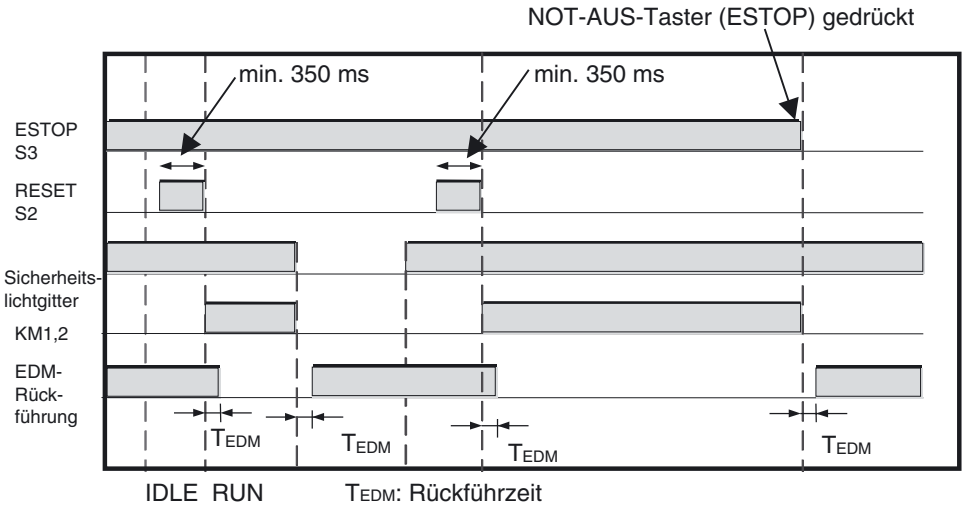
S3: NOT-AUS-Taster

KM1 und KM2: Schütze

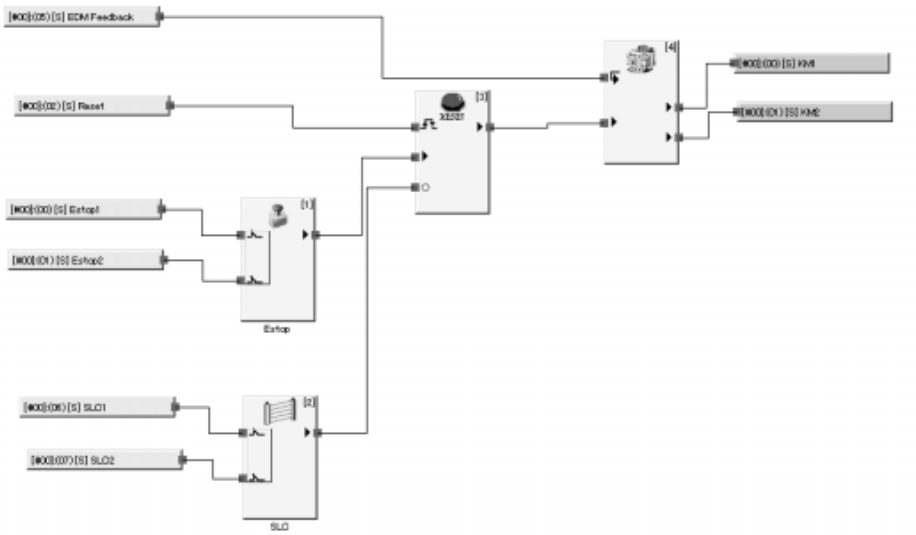
Hinweis (1) Schließen Sie die Klemmen V0 und G0 (Spannungsversorgung für interne Schaltkreise) an eine 24-V-DC-Spannungsversorgung an.

(2) Das Beispiel zeigt die Klemmenbelegung des Sicherheitsnetzwerk-Controllers NE1A-SCPU01(-V1).

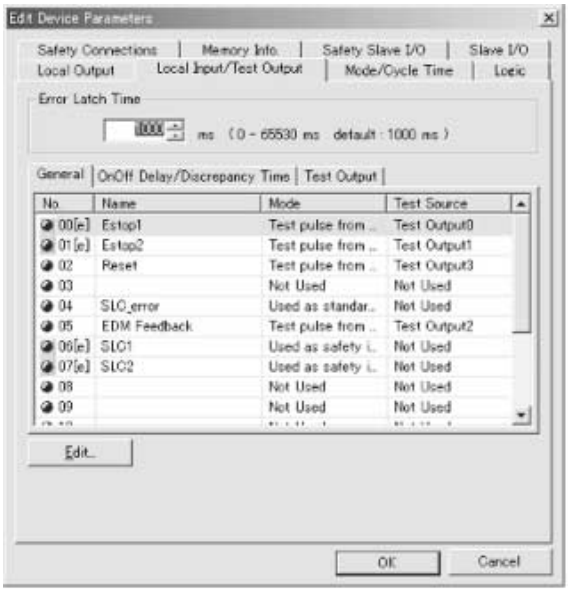
Zeitablaufdiagramm



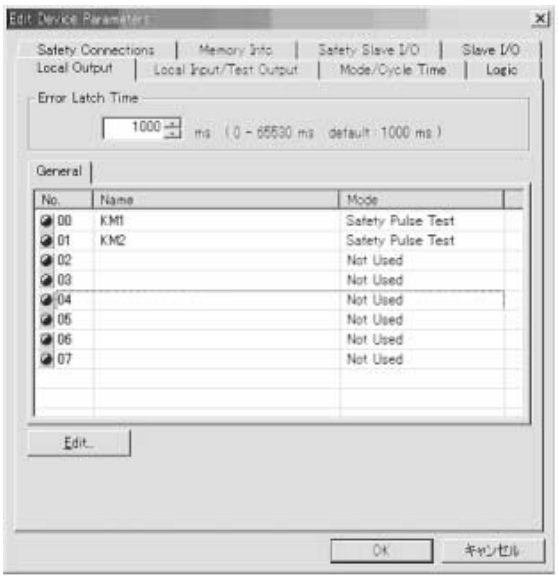
Programmierbeispiel



Lokale Eingänge / Testausgänge

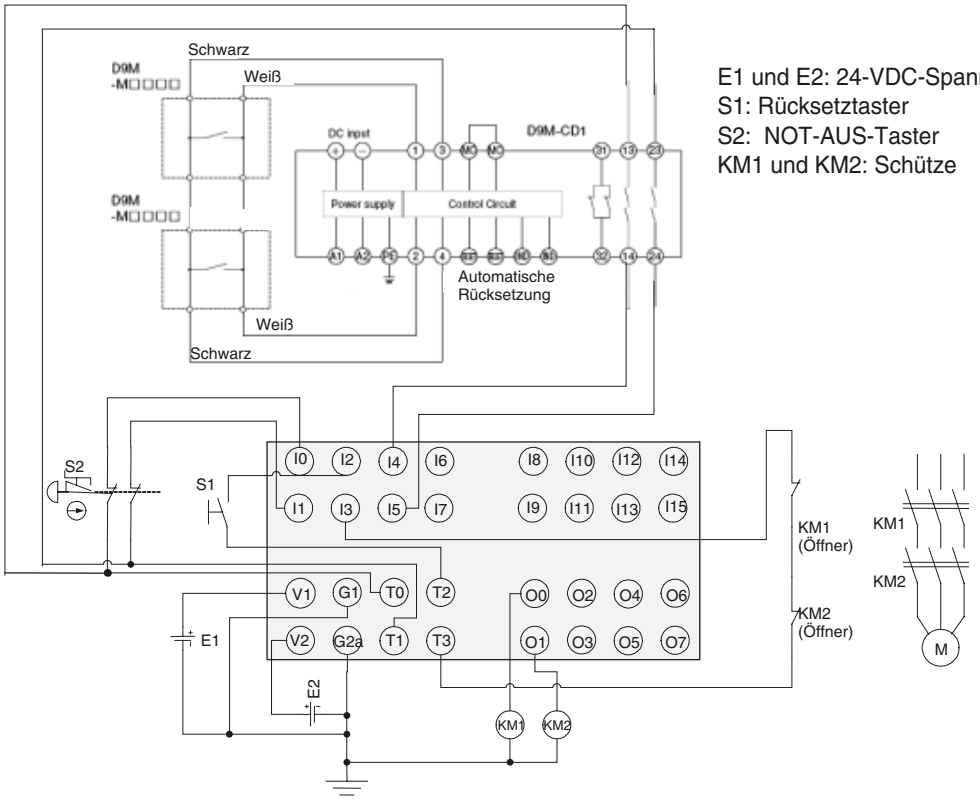


Lokale Ausgänge



A-1-5 Sicherheitsmatte: Zweikanal-Sicherheitsmatte mit manueller Rücksetzung und Zweikanal-NOT-AUS-Taster mit manueller Rücksetzung

Verdrahtungsbeispiel

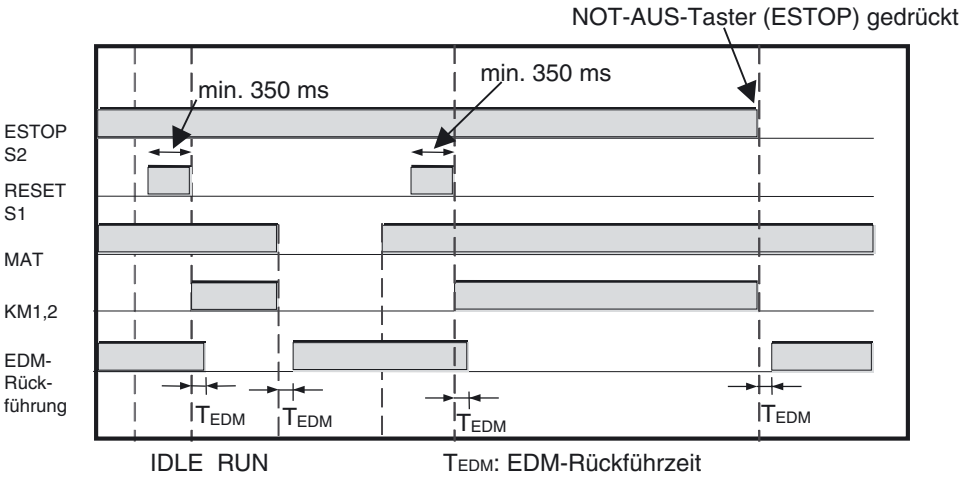


E1 und E2: 24-VDC-Spannungsversorgung
S1: Rücksetztaster
S2: NOT-AUS-Taster
KM1 und KM2: Schütze

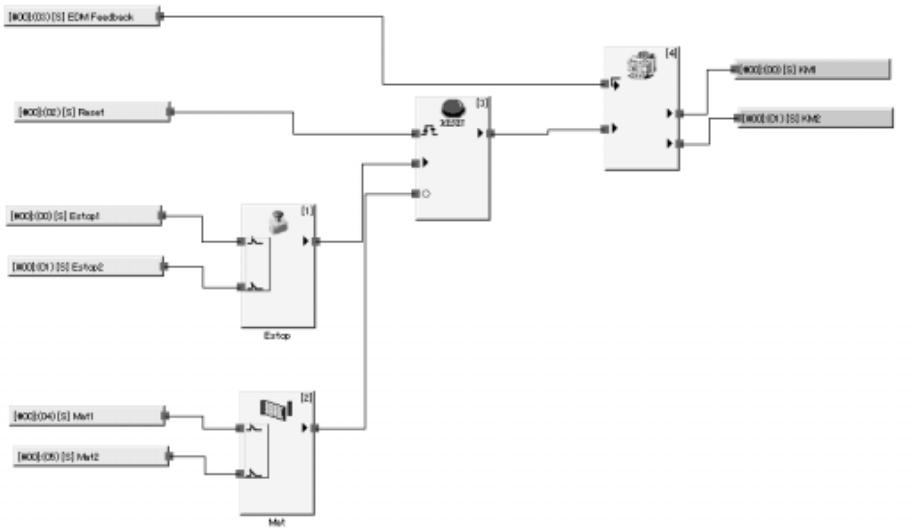
Hinweis (1) Schließen Sie die Klemmen V0 und G0 (Spannungsversorgung für interne Schaltkreise) an eine 24-V-DC-Spannungsversorgung an.

(2) Das Beispiel zeigt die Klemmenbelegung des Sicherheitsnetzwerk-Controllers NE1A-SCPU01(-V1).

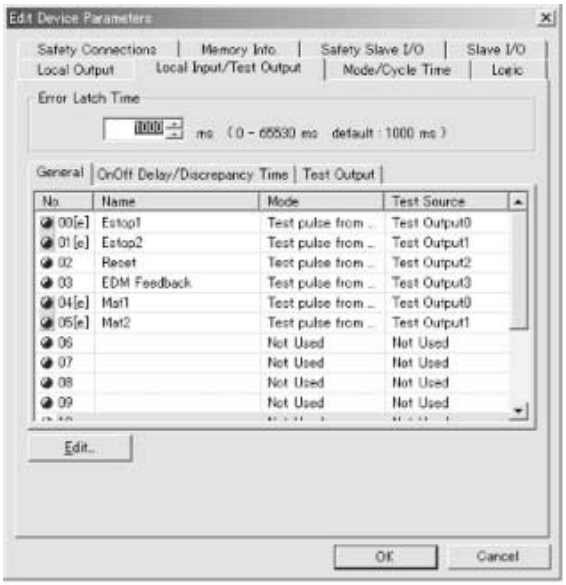
Zeitablaufdiagramm



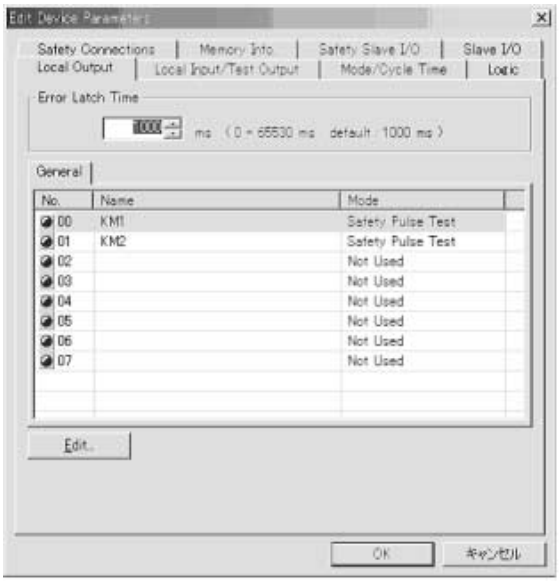
Programmierbeispiel



Lokale Eingänge / Testausgänge



Lokale Ausgänge



Anhang 2: Berechnete Werte für PFD und PFH

Die nachstehenden Tabellen enthalten die berechneten Werte für PFD und PFH für den Sicherheitsnetzwerk-Controller NE1A. Diese Werte müssen für alle Geräte innerhalb des Systems berechnet werden, um der erforderlichen SIL-Stufe für die Anwendung zu entsprechen.

A-2-1 Berechnete PFD-Werte

Modell	Testintervall (Jahre)	PFD
NE1A-SCPU01(-V1)	0,25	4,68E-07
	0,5	9,32E-07
	1	1,86E-06
	2	3,72E-06
NE1A-SCPU02	0,25	5,90E-07
	0,5	1,17E-07
	1	2,34E-06
	2	4,68E-06

A-2-2 Berechnete PFH-Werte

Modell	PFH
NE1A-SCPU01(-V1)	4,25E-10
NE1A-SCPU02	5,39E-10

Anhang 3: DeviceNet Explicit Messages

Benutzerspezifizierte NE1A Parameter können gelesen und geschrieben werden, indem DeviceNet Explicit Messages an den Sicherheitsnetzwerk-Controller NE1A übermittelt werden. Darauf hin verarbeitet der Sicherheitsnetzwerk-Controller NE1A die empfangenen Meldungen und übermittelt Rückmeldungen. Dieser Anhang beschreibt die vom Sicherheitsnetzwerk-Controller NE1A unterstützten Meldungen.

A-3-1 Explicit Messages: NE1A-SCPU01-V1

Allgemeinen Status lesen: NE1A-SCPU01-V1

Explicit Message	Dienst	Funktion	Befehl					Antwort
			Service-code	ClassI D	Instance -ID	Attribut-ID	Daten-größe	
Read Unit General Status	Lesen	Liest den allgemeinen Status der Baugruppe.	0E hex	39 (hex)	01 (hex)	6E hex	---	1 Byte

E/A-Bereich lesen: NE1A-SCPU01-V1

Explicit Message	Dienst	Funktion	Befehl					Antwort
			Service-code	Class ID	Instance -ID	Attribut-ID	Daten-größe	
Read I/O Area	Lesen	Liest den E/A-Bereich der Baugruppe. Instance-ID-Spezifikationsbereich: Lokaler Eingang = 01 Lokaler Ausgang/Testausgang = 02 Sicherheitseingang = 05 Sicherheitsausgang = 06 Adress-Spezifikationsbereich: Lokaler Eingang: 0 oder 1 Lokaler Ausgang/Testausgang: 0 oder 1 Sicherheitseingang: 0 bis 511 Sicherheitsausgang: 0 bis 511	0E hex	306 (hex)	01, 02, 05 oder 06 hex	---	Erstes und zweites Byte Offset-Adresse: 0000 bis 01FF hex 0 bis 511 Drittes und viertes Byte Lesegröße: 0001 bis 0100 hex (1 bis 256)	Lesedaten

Einstellen und Überwachen von Sicherheitseingangsklemmen: Eingänge (NE1A-SCPU01-V1)

Explicit Message	Dienst	Funktion	Befehl					Antwort
			Service-code	Class ID	In-stance-ID	Attri-but-ID	Datengröße	
Monitor Mode for Terminal Maintenance Information	Lesen	Liest den Überwachungsmodus der Wartungsinformationen für den durch die Instanz-ID spezifizierten Eingang (1 bis 16).	0E hex	3D hex	01 bis 10 hex	65 (hex)	---	1 Byte 00 hex: Gesamteinschaltdauer-Modus 01 hex: Schalthäufigkeitszähler-Modus
	Schreiben	Schreibt den Überwachungsmodus der Wartungsinformationen für den durch die Instanz-ID spezifizierten Eingang (1 bis 16).	10 (hex)	3D hex	01 bis 10 hex	65 (hex)	1 Byte 00 hex: Gesamteinschaltdauer-Modus 01 hex: Schalthäufigkeitszähler-Modus	---
SV for Input Total ON Time or Contact Operation Counter	Lesen	Liest den Sollwert für Gesamteinschaltdauer (Einheit: Sekunden) oder Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Eingang (1 bis 16).	0E hex	3D hex	01 bis 10 hex	68 (hex)	---	4 Bytes 0000 0000 bis FFFF FFFF hex (0 bis 4.294.967.295)
	Schreiben	Schreibt den Sollwert für Gesamteinschaltdauer (Einheit: Sekunden) oder Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Eingang (1 bis 16).	10 (hex)	3D hex	01 bis 10 hex	68 (hex)	4 Bytes 0000 0000 bis FFFF FFFF hex (0 bis 4,294,967,295)	---
Read Input Total ON Time or Contact Operation Counter	Lesen	Liest die Gesamteinschaltdauer (Einheit: Sekunden) oder den Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Eingang (1 bis 16).	0E hex	3D hex	01 bis 10 hex	66 (hex)	---	4 Bytes 0000 0000 bis FFFF FFFF hex (0 bis 4.294.967.295)
Reset Input Total ON Time or Contact Operation Counter	Reset	Setzt die Gesamteinschaltdauer (Einheit: Sekunden) oder den Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Eingang (1 bis 16) auf 0 zurück.	05 (hex)	3D hex	01 bis 10 hex	66 (hex)	---	---
Read Monitor Status of Input Total ON Time or Contact Operation Counter	Lesen	Liest den Überwachungsstatus der Gesamteinschaltdauer oder des Schalthäufigkeitszählers für den über die Instanz-ID spezifizierten Eingang (1 bis 16).	0E hex	3D hex	01 bis 10 hex	67 (hex)	?	1 Byte 00 hex: im Sollbereich 01 hex: nicht im Sollbereich (über dem Überwachungswert)
Read Safety Input Normal Flag	Lesen	Liest den Status des über die Instanz-ID spezifizierten Normal-Merkers (1 bis 16).	0E hex	3D hex	01 bis 10 hex	04 (hex)	?	1 Byte 00 hex: Fehler 01 hex: Normal
Read Safety Input Error Information Cause	Lesen	Liest die Ursache für die Deaktivierung (AUS) des über die Instanz-ID spezifizierten Normal-Merkers (1 bis 16).	0E hex	3D hex	01 bis 10 hex	6E hex	---	1 Byte 00 hex: Kein Fehler 01 hex: Ungültige Konfiguration 02 hex: Testsignalfehler 03 hex: Interner Schaltkreisfehler 04 hex: Diskrepanzfehler 05 hex: Fehler im anderen von zwei Kanälen
Read AND of Safety Input Normal Flags	Lesen	Liest das logische AND des Normal-Merker-Status für alle Eingänge (1 bis 16).	0E hex	3E hex	01 (hex)	05 (hex)	---	1 Byte 00 hex: Fehler 01 hex: Alle normal
Read OR of Monitor Status of Input Total ON Times or Contact Operation Counters	Lesen	Liest das logische OR des Überwachungsstatus der Gesamteinschaltdauer oder des Schalthäufigkeitszählers für alle Eingänge (1 bis 16).	0E hex	3E hex	01 (hex)	72 (hex)	---	1 Byte 00 hex: Alle im Sollbereich 01 hex: Eingang nicht im Sollbereich (über dem Überwachungswert)

Einstellen und Überwachen von Sicherheitsausgangsklemmen: Ausgänge (NE1A-SCPU01-V1)

Explicit Message	Dienst	Funktion	Befehl					Antwort
			Service-code	Class ID	In-stance-ID	Attri-but-ID	Datengröße	
Monitor Mode for Terminal Maintenance Information	Lesen	Liest den Überwachungsmodus der Wartungsinformationen für den über die Instanz-ID spezifizierten Ausgang (1 bis 8).	0E hex	3B hex	01 bis 08 hex	65 (hex)	---	1 Byte 00 hex: Gesamteinschaltdauer-Modus 01 hex: Schalthäufigkeitszähler-Modus
	Schreiben	Schreibt den Überwachungsmodus der Wartungsinformationen für den über die Instanz-ID spezifizierten Ausgang (1 bis 8).	10 (hex)	3B hex	01 bis 08 hex	65 (hex)	1 Byte 00 hex: Gesamteinschaltdauer-Modus 01 hex: Schalthäufigkeitszähler-Modus	---
SV for Output Total ON Time or Contact Operation Counter	Lesen	Liest den Sollwert für Gesamteinschaltdauer (Einheit: Sekunden) oder Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Eingang (1 bis 8).	0E hex	3B hex	01 bis 08 hex	68 (hex)	---	4 Bytes 0000 0000 bis FFFF FFFF hex (0 bis 4.294.967.295)
	Schreiben	Schreibt den Sollwert für Gesamteinschaltdauer (Einheit: Sekunden) oder Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Eingang (1 bis 8).	10 (hex)	3B hex	01 bis 08 hex	68 (hex)	4 Bytes 0000 0000 bis FFFF FFFF hex (0 bis 4,294,967,295)	---
Read Output Total ON Time or Contact Operation Counter	Lesen	Liest die Gesamteinschaltdauer (Einheit: Sekunden) oder den Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Eingang (1 bis 8).	0E hex	3B hex	01 bis 08 hex	66 (hex)	---	4 Bytes 0000 0000 bis FFFF FFFF hex (0 bis 4.294.967.295)
Reset Output Total ON Time or Contact Operation Counter	Reset	Setzt die Gesamteinschaltdauer (Einheit: Sekunden) oder den Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Ausgang (1 bis 8) auf 0 zurück.	05 (hex)	3B hex	01 bis 08 hex	66 (hex)	---	---
Read Monitor Status of Output Total ON Time or Contact Operation Counter	Lesen	Liest den Überwachungsstatus der Gesamteinschaltdauer oder Schalthäufigkeit für den über die Instanz-ID spezifizierten Ausgang (1 bis 8).	0E hex	3B hex	01 bis 08 hex	67 (hex)	---	1 Byte 00 hex: im Sollbereich 01 hex: nicht im Sollbereich (über dem Überwachungswert)
Read Safety Output Normal Flag	Lesen	Liest den Status des über die Instanz-ID spezifizierten Normal-Merkers (1 bis 8).	0E hex	3B hex	01 bis 08 hex	05 (hex)	---	1 Byte 00 hex: Fehler 01 hex: Normal
Read Safety Output Error Information Cause	Lesen	Liest die Ursache für die Deaktivierung (AUS) des über die Instanz-ID spezifizierten Normal-Merkers (1 bis 8).	0E hex	3B hex	01 bis 08 hex	6E hex	---	1 Byte 00 hex: Kein Fehler 01 hex: Ungültige Konfiguration 02 hex: Überstrom-Erkennung 03 hex: Kurzschluss-Erkennung 04 hex: Hochkonstanter Fehler 05 hex: Fehler im anderen von zwei Kanälen 06 hex: Interner Relaiskreisfehler 07 hex: Relaisfehler 08 hex: Datenfehler zwischen Zweikanal-Ausgängen 09 hex: Kurzschlusserkennung zwischen Kabeln
Read AND of Safety Output a Normal Flags	Lesen	Liest das logische AND aller Ausgänge (1 bis 8).	0E hex	3C hex	01 (hex)	05 (hex)	---	1 Byte 00 hex: Fehler 01 hex: Alle normal
Read OR of Monitor Status of Output Total ON Times or Contact Operation Counters	Lesen	Liest das logische OR des Überwachungsstatus der Gesamteinschaltdauer oder des Schalthäufigkeitszählers für alle Ausgänge (1 bis 8).	0E hex	3C hex	01 (hex)	72 (hex)	---	1 Byte 00 hex: Alle im Sollbereich 01 hex: Ausgang nicht im Sollbereich (über dem Überwachungswert)

Überwachung von Testausgangsklemmen: NE1A-SCPU01-V1

Explicit Message	Dienst	Funktion	Befehl					Antwort
			Service-code	Class ID	In-stance-ID	Attri-but-ID	Datengröße	
Monitor Mode for Terminal Maintenance Information	Lesen	Liest den Überwachungsmodus der Wartungsinformationen des über die Instanz-ID spezifizierten Testausgangs (1 bis 4).	0E hex	307 (hex)	01 bis 04 hex	83 (hex)	---	1 Byte 00 hex: Gesamteinschaltdauer-Modus 01 hex: Schalthäufigkeitszähler-Modus
	Schreiben	Schreibt den Überwachungsmodus der Wartungsinformationen des über die Instanz-ID spezifizierten Testausgangs (1 bis 4).	10 (hex)	307 (hex)	01 bis 04 hex	83 (hex)	1 Byte 00 hex: Gesamteinschaltdauer-Modus 01 hex: Schalthäufigkeitszähler-Modus	---
SV for Test Output Total ON Time or Contact Operation Counter	Lesen	Liest den Sollwert für Gesamteinschaltdauer (Einheit: Sekunden) oder Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Eingang (1 bis 4).	0E hex	307 (hex)	01 bis 04 hex	86 (hex)	---	4 Bytes 0000 0000 bis FFFF FFFF hex (0 bis 4,294,967,295)
	Schreiben	Schreibt den Sollwert für Gesamteinschaltdauer (Einheit: Sekunden) oder Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Eingang (1 bis 4).	10 (hex)	307 (hex)	01 bis 04 hex	86 (hex)	4 Bytes 0000 0000 bis FFFF FFFF hex (0 bis 4,294,967,295)	---
Read Test Output Total ON Time or Contact Operation Counter	Lesen	Liest die Gesamteinschaltdauer (Einheit: Sekunden) oder den Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Eingang (1 bis 16).	0E hex	307 (hex)	01 bis 04 hex	84 (hex)	---	4 Bytes 0000 0000 bis FFFF FFFF hex (0 bis 4,294,967,295)
Reset Test Output Total ON Time or Contact Operation Counter	Reset	Setzt die Gesamteinschaltdauer (Einheit: Sekunden) oder den Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Testausgang (1 bis 4) auf 0 zurück.	05 (hex)	307 (hex)	01 bis 04 hex	84 (hex)	---	---
Read Monitor Status of Test Output Total ON Time or Contact Operation Counter	Lesen	Liest den Überwachungsstatus der Gesamteinschaltdauer oder des Schalthäufigkeitszählers des über die Instanz-ID spezifizierten Testausgangs (1 bis 4).	0E hex	307 (hex)	01 bis 04 hex	85 (hex)	---	1 Byte 00 hex: im Sollbereich 01 hex: nicht im Sollbereich (über dem Überwachungswert)
Read Test Output Safety Flag	Lesen	Liest den Status des Normal-Merkers für den über die Instanz-ID spezifizierten Testausgang (1 bis 4).	0E hex	307 (hex)	01 bis 04 hex	68 (hex)	---	1 Byte 00 hex: Normal 01 hex: Fehler
Read Test Output Error Information Cause	Lesen	Liest die Ursache für die Deaktivierung (AUS) des Normal-Merkers für den über die Instanz-ID spezifizierten Testausgang (1 bis 4).	0E hex	307 (hex)	01 bis 04 hex	76 (hex)	---	1 Byte 00 hex: Kein Fehler 01 hex: Ungültige Konfiguration 02 hex: Überstrom-Erkennung 05 hex: Hochkonstanter Fehler 06 hex: Unterstrom-Erkennung
Read OR of Test Output Safety Flags	Lesen	Liest das logische OR des Normal-Merker-Status für alle Testausgänge (1 bis 4).	0E hex	308 (hex)	01 (hex)	69 (hex)	---	1 Byte 00 hex: Alle normal 01 hex: Fehler
Read OR of Monitor Status of Test Output Total ON Times or Contact Operation Counters	Lesen	Liest das logische OR des Überwachungsstatus der Gesamteinschaltdauer oder des Schalthäufigkeitszählers für alle Testausgänge (1 bis 4).	0E hex	308 (hex)	01 (hex)	72 (hex)	---	1 Byte 00 hex: Alle im Sollbereich 01 hex: Testausgang nicht im Sollbereich (über dem Überwachungswert)

A-3-2 Explicit Messages: NE1A-SCPU02

Allgemeinen Status lesen: NE1A-SCPU02

Explicit Message	Dienst	Funktion	Befehl					Antwort
			Service-code	Class ID	Instance-ID	Attribut-ID	Datengröße	
Read Unit General Status	Lesen	Liest den allgemeinen Status der Baugruppe.	0E hex	39 (hex)	01 (hex)	6E hex	---	1 Byte

E/A-Bereich lesen: NE1A-SCPU02

Explicit Message	Dienst	Funktion	Befehl					Antwort
			Service-code	Class ID	Instance-ID	Attribut-ID	Datengröße	
Read I/O Area	Lesen	Liest den E/A-Bereich der Baugruppe. Instance-ID-Spezifikationsbereich: Lokaler Eingang = 01 Lokaler Ausgang/Testausgang = 02 Sicherheitseingang = 05 Sicherheitsausgang = 06 Adress-Spezifikationsbereich: Lokaler Eingang: 0 bis 4 Lokaler Ausgang/Testausgang: 0 oder 1 Sicherheitseingang: 0 bis 511 Sicherheitsausgang: 0 bis 511	4B hex	306 (hex)	01, 02, 05 und 06 hex	---	Erstes und zweites Byte Offset-Adresse: 0000 bis 01FF hex (0 bis 511), Drittes und viertes Byte Lesegröße: 0001 bis 0100 hex (1 bis 256)	Lesedaten

Einstellen und Überwachen von Sicherheitseingangsklemmen: Eingänge (NE1A-SCPU02)

Explicit Message	Dienst	Funktion	Befehl					Antwort
			Service-code	Class ID	In-stance-ID	Attri-but-ID	Datengröße	
Monitor Mode for Terminal Maintenance Information	Lesen	Liest den Überwachungsmodus der Wartungsinformationen für den durch die Instanz-ID spezifizierten Eingang (1 bis 40).	0E hex	3D hex	01 bis 28 hex	65 (hex)	---	1 Byte 00 hex: Gesamteinschaltdauer-Modus 01 hex: Schalthäufigkeitszähler-Modus
	Schreiben	Schreibt den Überwachungsmodus der Wartungsinformationen für den durch die Instanz-ID spezifizierten Eingang (1 bis 40).	10 (hex)	3D hex	01 bis 28 hex	65 (hex)	1 Byte 00 hex: Gesamteinschaltdauer-Modus 01 hex: Schalthäufigkeitszähler-Modus	---
SV for Input Total ON Time or Contact Operation Counter	Lesen	Liest den Sollwert für Gesamteinschaltdauer (Einheit: Sekunden) oder Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Eingang (1 bis 40).	0E hex	3D hex	01 bis 28 hex	68 (hex)	---	4 Bytes 0000 0000 bis FFFF FFFF hex (0 bis 4,294,967,295)
	Schreiben	Schreibt den Sollwert für Gesamteinschaltdauer (Einheit: Sekunden) oder Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Eingang (1 bis 40).	10 (hex)	3D hex	01 bis 28 hex	68 (hex)	4 Bytes 0000 0000 bis FFFF FFFF hex (0 bis 4,294,967,295)	---
Read Input Total ON Time or Contact Operation Counter	Lesen	Liest die Gesamteinschaltdauer (Einheit: Sekunden) oder den Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Eingang (1 bis 40).	0E hex	3D hex	01 bis 28 hex	66 (hex)	---	4 Bytes 0000 0000 bis FFFF FFFF hex (0 bis 4,294,967,295)
Reset Input Total ON Time or Contact Operation Counter	Reset	Setzt die Gesamteinschaltdauer (Einheit: Sekunden) oder den Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Eingang (1 bis 40) auf 0 zurück.	05 (hex)	3D hex	01 bis 28 hex	66 (hex)	---	---
Read Monitor Status of Input Total ON Time or Contact Operation Counter	Lesen	Liest den Überwachungsstatus der Gesamteinschaltdauer oder des Schalthäufigkeitszählers für den über die Instanz-ID spezifizierten Eingang (1 bis 40).	0E hex	3D hex	01 bis 28 hex	67 (hex)	---	1 Byte 00 hex: im Sollbereich 01 hex: nicht im Sollbereich (über dem Überwachungswert)
Read Safety Input Normal Status	Lesen	Liest den Status des über die Instanz-ID spezifizierten Normal-Merkers (1 bis 40).	0E hex	3D hex	01 bis 28 hex	04 (hex)	---	1 Byte 00 hex: Fehler 01 hex: Normal
Read Safety input Error Information Cause	Lesen	Liest die Ursache für die Deaktivierung (AUS) des über die Instanz-ID spezifizierten Normal-Merkers (1 bis 40).	0E hex	3D hex	01 bis 28 hex	6E hex	---	1 Byte 00 hex: Kein Fehler 01 hex: Ungültige Konfiguration 02 hex: Testsignalfehler 03 hex: Interner Schaltkreisfehler 04 hex: Diskrepanzfehler 05 hex: Fehler im anderen von zwei Kanälen
Read AND of Safety Input Normal Flags	Lesen	Liest das logische AND des Normal-Merker-Status für alle Eingänge (1 bis 40).	0E hex	3E hex	01 (hex)	05Hex	---	1 Byte 00 hex: Fehler 01 hex: Alle normal
Read OR of Monitor Status of Input Total ON Times or Contact Operation Counters	Lesen	Liest das logische OR des Überwachungsstatus der Gesamteinschaltdauer oder des Schalthäufigkeitszählers für alle Eingänge (1 bis 40).	0EHex	3EHex	01 (hex)	72Hex	---	1 Byte 00 hex: Alle im Sollbereich 01 hex: Eingang nicht im Sollbereich (über dem Überwachungswert)

Einstellen und Überwachen von Sicherheitsausgangsklemmen: Ausgänge (NE1A-SCPU02)

Explicit Message	Dienst	Funktion	Befehl					Antwort
			Service-code	Class ID	In-stance-ID	Attri-but-ID	Datengröße	
Monitor Mode for Terminal Maintenance Information	Lesen	Liest den Überwachungsmodus der Wartungsinformationen für den über die Instanz-ID spezifizierten Ausgang (1 bis 8).	0E hex	3B hex	01 bis 08 hex	65 (hex)	---	1 Byte 00 hex: Gesamteinschaltdauer-Modus 01 hex: Schalthäufigkeitszähler-Modus
	Schreiben	Schreibt den Überwachungsmodus der Wartungsinformationen für den über die Instanz-ID spezifizierten Ausgang (1 bis 8).	10 (hex)	3B hex	01 bis 08 hex	65 (hex)	1 Byte 00 hex: Gesamteinschaltdauer-Modus 01 hex: Schalthäufigkeitszähler-Modus	---
SV for Output Total ON Time or Contact Operation Counter	Lesen	Liest den Sollwert für Gesamteinschaltdauer (Einheit: Sekunden) oder Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Ausgang (1 bis 8).	0E hex	3B hex	01 bis 08 hex	68 (hex)	---	4 Bytes 0000 0000 bis FFFF FFFF hex (0 bis 4,294,967,295)
	Schreiben	Liest den Sollwert für Gesamteinschaltdauer (Einheit: Sekunden) oder Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Ausgang (1 bis 8).	10 (hex)	3B hex	01 bis 08 hex	68 (hex)	4 Bytes 0000 0000 bis FFFF FFFF hex (0 bis 4.294.967.295)	---
Read Output Total ON Time or Contact Operation Counter	Lesen	Liest die Gesamteinschaltdauer (Einheit: Sekunden) oder den Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Ausgang (1 bis 8).	0E hex	3B hex	01 bis 08 hex	66 (hex)	---	4 Bytes 0000 0000 bis FFFF FFFF hex (0 bis 4,294,967,295)
Reset Output Total ON Time or Contact Operation Counter	Reset	Setzt die Gesamteinschaltdauer (Einheit: Sekunden) oder den Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Ausgang (1 bis 8) auf 0 zurück.	05 (hex)	3B hex	01 bis 08 hex	66 (hex)	---	---
Read Monitor Status of Output Total ON Time or Contact Operation Counter	Lesen	Liest den Überwachungsstatus der Gesamteinschaltdauer oder Schalthäufigkeit für die über die Instanz-ID spezifizierte Nummer (1 bis 8).	0E hex	3B hex	01 bis 08 hex	67 (hex)	---	1 Byte 00 hex: im Sollbereich 01 hex: nicht im Sollbereich (über dem Überwachungswert)
Read Safety Output Normal Flag	Lesen	Liest den Status des über die Instanz-ID spezifizierten Normal-Merkers (1 bis 8).	0E hex	3B hex	01 bis 08 hex	05 (hex)	---	1 Byte 00 hex: Fehler 01 hex: Normal
Read Safety Output Error Information Cause	Lesen	Liest die Ursache für die Deaktivierung (AUS) des über die Instanz-ID spezifizierten Normal-Merkers (1 bis 8).	0E hex	3B hex	01 bis 08 hex	6E hex	---	1 Byte 00 hex: Kein Fehler 01 hex: Ungültige Konfiguration 02 hex: Überstrom-Erkennung 03 hex: Kurzschluss-Erkennung 04 hex: Hochkonstanter Fehler 05 hex: Fehler im anderen von zwei Kanälen 06 hex: Interner Relaiskreisfehler 07 hex: Relaisfehler 08 hex: Datenfehler zwischen Zweikanal-Ausgängen 09 hex: Kurzschlusserkennung zwischen Kabeln
Read AND of Safety Output Normal Flags	Lesen	Liest das logische AND des Normal-Merker-Status für alle Ausgänge (1 bis 8).	0E hex	3C hex	01 (hex)	05 (hex)	---	1 Byte 00 hex: Fehler 01 hex: Alle normal
Read OR of Monitor Status of Output Total ON Times or Contact Operation Counters	Lesen	Liest das logische OR des Überwachungsstatus der Gesamteinschaltdauer oder des Schalthäufigkeitszählers für alle Ausgänge (1 bis 8).	0E hex	3C hex	01 (hex)	72 (hex)	---	1 Byte 00 hex: Alle im Sollbereich 01 hex: Ausgang nicht im Sollbereich (über dem Überwachungswert)

Überwachung von Testausgangsklemmen: NE1A-SCPU02

Explicit Message	Dienst	Funktion	Befehl					Antwort
			Service-code	Class ID	In-stance-ID	Attri-but-ID	Datengröße	
Monitor Mode for Terminal Maintenance Information	Lesen	Liest den Überwachungsmodus der Wartungsinformationen den über die Instanz-ID spezifizierten Testausgang (1 bis 8).	0E hex	307 (hex)	01 bis 08 hex	83 (hex)	---	1 Byte 00 hex: Gesamteinschaltdauer-Modus 01 hex: Schalthäufigkeitszähler-Modus
	Schreiben	Schreibt den Überwachungsmodus der Wartungsinformationen für den über die Instanz-ID spezifizierten Testausgang (1 bis 8).	10 (hex)	307 (hex)	01 bis 08 hex	83 (hex)	1 Byte 00 hex: Gesamteinschaltdauer-Modus 01 hex: Schalthäufigkeitszähler-Modus	---
SV for Test Output Total ON Time or Contact Operation Counter	Lesen	Liest den Sollwert für Gesamteinschaltdauer (Einheit: Sekunden) oder Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Testausgang (1 bis 8).	0E hex	307 (hex)	01 bis 08 hex	86 (hex)	---	4 Bytes 0000 0000 bis FFFF FFFF hex (0 bis 4.294.967.295)
	Schreiben	Schreibt den Sollwert für Gesamteinschaltdauer (Einheit: Sekunden) oder Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Testausgang (1 bis 8).	10 (hex)	307 (hex)	01 bis 08 hex	86 (hex)	4 Bytes 0000 0000 bis FFFF FFFF hex (0 bis 4.294.967.295)	---
Read Test Output for Total ON Time or Contact Operation Counter	Lesen	Liest die Gesamteinschaltdauer (Einheit: Sekunden) oder den Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Testausgang (1 bis 8).	0E hex	307 (hex)	01 bis 08 hex	84 (hex)	---	4 Bytes 0000 0000 bis FFFF FFFF hex (0 bis 4.294.967.295)
Reset Test Output for Total ON Time or Contact Operation Counter	Reset	Setzt die Gesamteinschaltdauer (Einheit: Sekunden) oder den Schalthäufigkeitszähler (Einheit: Schaltspiele) für den über die Instanz-ID spezifizierten Testausgang (1 bis 8) auf 0 zurück.	05 (hex)	307 (hex)	01 bis 08 hex	84 (hex)	---	---
Read Monitor Status of Test Output Total ON Time or Contact Operation Counter	Lesen	Liest den Überwachungsstatus der Gesamteinschaltdauer oder des Schalthäufigkeitszählers für den über die Instanz-ID spezifizierten Testausgang (1 bis 8).	0E hex	307 (hex)	01 bis 08 hex	85 (hex)	---	1 Byte 00 hex: im Sollbereich 01 hex: nicht im Sollbereich (über dem Überwachungswert)
Read Test Output Normal Flag	Lesen	Liest den Status des Normal-Merkers für den über die Instanz-ID spezifizierten Testausgang (1 bis 8).	0E hex	307 (hex)	01 bis 08 hex	68 (hex)	---	1 Byte 00 hex: Normal 01 hex: Fehler
Read Test Output Error Information Cause	Lesen	Liest die Ursache für die Deaktivierung (AUS) des Normal-Merkers für den über die Instanz-ID spezifizierten Testausgang (1 bis 8).	0E hex	307 (hex)	01 bis 08 hex	76 (hex)	---	1 Byte 00 hex: Kein Fehler 01 hex: Ungültige Konfiguration 02 hex: Überstrom-Erkennung 05 hex: Hochkonstanter Fehler 06 hex: Unterstrom-Erkennung
Read OR of Test Output Normal Flags	Lesen	Liest den Normal-Merker-Status aller Testausgänge (1 bis 8).	0E hex	308 (hex)	01 (hex)	69 (hex)	---	1 Byte 00 hex: Alle normal 01 hex: Fehler
Read OR of Monitor Status of Test Output Total ON Times or Contact Operation Counters	Lesen	Liest das logische OR des Überwachungsstatus der Gesamteinschaltdauer oder des Schalthäufigkeitszählers für alle Testausgänge (1 bis 8).	0E hex	308 (hex)	01 (hex)	72 (hex)	---	1 Byte 00 hex: Alle im Sollbereich 01 hex: Testausgang nicht im Sollbereich (über dem Überwachungswert)

A-3-3 Explicit Messages: NE1A-SCPU01

Allgemeinen Status lesen: NE1A-SCPU01

Explicit Message	Dienst	Funktion	Befehl					Antwort
			Service-code	Class ID	In-stance-ID	Attri-but-ID	Datengröße	
Read Unit General Status	Lesen	Liest den allgemeinen Status der Baugruppe.	0E hex	39 (hex)	01 (hex)	6E hex	---	1 Byte

E/A-Bereich lesen: NE1A-SCPU01

Explicit Message	Dienst	Funktion	Befehl					Antwort
			Service-code	Class ID	In-stance-ID	Attri-but-ID	Datengröße	
Read I/O Area	Lesen	Liest den E/A-Bereich der Baugruppe. Instance-ID-Spezifikationsbereich: Lokaler Eingang = 01 Lokaler Ausgang/Testausgang = 02 Sicherheitseingang = 05 Sicherheitsausgang = 06 Adress-Spezifikationsbereich: Lokaler Eingang: 0 oder 1 Lokaler Ausgang/Testausgang: 0 oder 1 Sicherheitseingang: 0 bis 511 Sicherheitsausgang: 0 bis 511	4B hex	306 (hex)	01, 02, 05 und 06 hex	---	Erstes und zweites Byte Offset-Adresse: 0000 bis 01FF hex (0 bis 511), Drittes und viertes Byte Lesegröße: 0001 bis 0100 hex (1 bis 256)	Lesedaten

Einstellen und Überwachen von Sicherheitseingangsklemmen: Eingang (NE1A-SCPU01)

Explicit Message	Dienst	Funktion	Befehl					Antwort
			Service-code	Class ID	In-stance-ID	Attri-but-ID	Datengröße	
Read Safety Input Normal Flag	Lesen	Liest den normalen Status des über die Instanz-ID spezifizierten Normal-Merkers (1 bis 16).	0E hex	3D hex	01 bis 10 hex	04 (hex)	---	1 Byte 00 hex: Fehler 01 hex: Normal
Read Safety input Error Information Cause	Lesen	Liest die Ursache für die Deaktivierung (AUS) des über die Instanz-ID spezifizierten Normal-Merkers (1 bis 16).	0E hex	3D hex	01 bis 10 hex	6E hex	---	1 Byte 00 hex: Kein Fehler 01 hex: Ungültige Konfiguration 02 hex: Testsignalfehler 03 hex: Interner Schaltkreisfehler 04 hex: Diskrepanzfehler 05 hex: Fehler im anderen von zwei Kanälen
Read AND of Safety Input Normal Flags	Lesen	Liest das logische AND des Normal-Merker-Status für alle Eingänge (1 bis 16).	0E hex	3E hex	01 (hex)	05 (hex)	---	1 Byte 00 hex: Fehler 01 hex: Alle normal

Einstellen und Überwachen von Sicherheitsausgangsklemmen: Ausgänge (NE1A-SCPU01)

Explicit Message	Dienst	Funktion	Befehl					Antwort
			Service - Code	Class ID	In-stance -ID	Attri-but-ID	Datengröße	
Read Safety Output Normal Flag	Lesen	Liest den Status des über die Instanz-ID spezifizierten Normal-Merkers (1 bis 8).	0E hex	3B hex	01 bis 08 hex	05 (hex)	---	1 Byte 00 hex: Fehler 01 hex: Normal
Read Safety Output Error Information Cause	Lesen	Liest die Ursache für die Deaktivierung (AUS, Fehler) des über die Instanz-ID spezifizierten Normal-Merkers (1 bis 8).	0E hex	3B hex	01 bis 08 hex	6E hex	---	1 Byte 00 hex: Kein Fehler 01 hex: Ungültige Konfiguration 02 hex: Überstrom-Erkennung 03 hex: Kurzschluss-Erkennung 04 hex: Hochkonstanter Fehler 05 hex: Fehler im anderen von zwei Kanälen 06 hex: Interner Relaiskreisfehler 07 hex: Relaisfehler 08 hex: Datenfehler zwischen Zweikanal-Ausgängen 09 hex: Kurzschlusserkennung zwischen Kabeln
Read AND of Safety Output Normal Flags	Lesen	Liest das logische AND des Normal-Merker-Status für alle Ausgänge (1 bis 8).	0E hex	3C hex	01 (hex)	05 (hex)	---	1 Byte 00 hex: Fehler 01 hex: Alle normal

Überwachung von Testausgangsklemmen: NE1A-SCPU01

Explicit Message	Dienst	Funktion	Befehl					Antwort
			Service-Code	Class ID	In-stance-ID	Attri-but-ID	Datengröße	
Read Test Output Normal Flag	Lesen	Liest den Status des Normal-Merkers des über die Instanz-ID spezifizierten Testausgangs (1 bis 4).	0E hex	307 (hex)	01 bis 04 hex	68 (hex)	---	1 Byte 00 hex: Normal 01 hex: Fehler
Read Test Output Error Information Cause	Lesen	Liest die Ursache für die Deaktivierung (AUS) des Normal-Merkers für den über die Instanz-ID spezifizierten Testausgang (1 bis 4).	0E hex	307 (hex)	01 bis 04 hex	76 (hex)	---	1 Byte 00 hex: Kein Fehler 01 hex: Ungültige Konfiguration 02 hex: Überstrom-Erkennung 05 hex: Hochkonstanter Fehler 06 hex: Unterstrom-Erkennung
Read OR of Test Output Normal Flags	Lesen	Liest das logische OR des Normal-Merker-Status für alle Ausgänge (1 bis 4).	0E hex	308 (hex)	01 (hex)	69 (hex)	---	1 Byte 00 hex: Alle normal 01 hex: Fehler

Glossar

Begriff	Definition
BusOff (Bus Aus)	Zustand, der beim Auftreten einer extrem hohen Kommunikationsfehlerrate eintreten kann. Wenn der interne Fehlerzähler einen bestimmten Grenzwert überschreitet, wird das Vorliegen eines Fehlers erkannt. (Der interne Fehlerzähler wird beim Starten oder Neustarten des Masters gelöscht. Bei Erhalt eines Normal-Frames wird er vermindert.)
DeviceNet Safety	Ein Sicherheitsnetzwerk, das DeviceNet um ein Sicherheitsprotokoll in Übereinstimmung mit SIL3 gemäß IEC61508 bis Steuerungskategorie 4 entsprechend EN954-1 erweitert.
Diskrepanzzeit	Der zeitliche Abstand zwischen der Änderung des Zustands eines von zwei Eingängen bis zur Änderung des Zustands des anderen Eingangs.
E/A-Konfiguration	In einem Gerät zu einer Gruppe zusammengefasste Daten, auf die von außerhalb des Geräts zugegriffen werden kann.
Einkanalmodus	Verwendung jeweils nur eines Eingangs bzw. Ausgangs als Eingang bzw. Ausgang.
EPI	Das Intervall der Sicherheitsdatenkommunikation zwischen dem Sicherheits-Master und dem Sicherheits-Slave.
Fault Present	Diverse Funktionsblöcke verfügen über „Fault Present“ als optionalen Ausgang. Dabei handelt es sich um einen Fehlerausgang, der besagt, dass der jeweilige Funktionsblock einen internen Logikfehler oder einen Eingangsdaten-Zeitfehler erkannt hat.
Fehlerhaltezeit	Die Zeitdauer, für die ein Fehlerzustand (Steuerungs- und Statusdaten, LED-Anzeigen) gehalten wird.
Konfiguration	Die Einstellungen für ein Gerät und ein Netzwerk.
Multicast-Verbindung	Sicherheits-E/A-Kommunikation in einer 1:n-Konfiguration (n = 1 bis 15).
Open Type (Parameter für die Vorgehensweise beim Herstellen der Verbindung)	Die Vorgehensweise beim Herstellen einer Sicherheitsverbindung. Der entsprechende Parameter in den Einstellungen des Sicherheits-Masters bietet drei mögliche Optionen.
PFD	Probability of Failure on Demand (Gefährliche Versagenswahrscheinlichkeit). Gibt die durchschnittliche Ausfallrate für eine System- oder Geräteanforderung an. Wird zur Berechnung des SIL (Safety Integrity Level) von Sicherheitssystemen verwendet.
PFH	Probability of Failure per hour (Wahrscheinlichkeit eines Ausfalls pro Stunde) Gibt die stündliche Ausfallrate für ein System oder Gerät an. Wird zur Berechnung des SIL (Safety Integrity Level) von Sicherheitssystemen verwendet.
Sicherheits-Controller (Sicherheits-SPS)	Eine für die Sicherheitssteuerung eingesetzte Steuerung hoher Zuverlässigkeit.
Sicherheitsdaten	Daten mit hoher Zuverlässigkeit und minimalem Risiko.
Sicherheitskette	Die logische Kette für die Aktualisierung einer Sicherheitsfunktion: Eingangsgerät (Sensor), Steuerungsgerät (einschließlich eines dezentralen E/A-Geräts) und Ausgangsgerät (Aktor).
Sicherheitsprotokoll	Die für die Einrichtung einer äußerst zuverlässigen Kommunikation hinzugefügte Kommunikationshierarchie.
Sicherheitssignatur	Ein vom Netzwerkkonfigurator an ein Gerät ausgegebenes Zertifikat der Konfigurationsdaten. Das Gerät verifiziert unter Verwendung der Sicherheitssignatur die Korrektheit der Konfigurationsdaten.
Singlecast-Verbindung	Sicherheits-E/A-Kommunikation in einer 1:1-Konfiguration.
Standard	Ein Gerät oder eine Gerätefunktion, bei dem/der keine Sicherheitsmaßnahmen zum Tragen kommen.
Testimpuls	Ein Signal, mit dem festgestellt wird, ob die externe Verdrahtung in Kontakt mit der Versorgungsspannung (+) steht oder ob Querschlüsse zwischen Signalleitungen bestehen
Verbindung	Logischer Kommunikationspfad für die Kommunikation zwischen Geräten.

Begriff	Definition
Zweikanaläquivalenzmodus	Variante des Zweikanalmodus, bei dem die logischen Zustände der beiden Eingänge bzw. Ausgänge äquivalent sind.
Zweikanalkomplementärmodus	Variante des Zweikanalmodus, bei dem die logischen Zustände der beiden Eingänge bzw. Ausgänge komplementär sind.
Zweikanalmodus	Verwendung von zwei Eingängen bzw. Ausgängen als redundante Eingänge bzw. Ausgänge.

Index

A

Abbruch, 22, 52, 55
Abbruchfehler, 200, 202
ABORT (Abbruch-Zustand), 182
Allgemeine Sicherheitshinweise, xviii
Allgemeiner Status, 76–77, 80–81
AND, 111, 117
Änderungen des Betriebsmodus, 185
Anschluss von Ausgangsgeräten, 43
Anschluss von Eingangsgeräten, 42
Attribute dezentraler E/A-Bereiche, 58
Ausgangspunkte-Einstellung, 115
Ausgangs-Tags, 109
Ausschaltverzögerungs-Zeitfunktion, 111, 148
Automatische Erkennung der Baudrate, 53

B

Baudrateneinstellung, 23, 53
Baudratenschalter, 23
Baugruppenstatus, 21, 55
Beispielberechnungen der Reaktionszeit, 194
Berechnete PFD-Werte, 242
Berechnete PFH-Werte, 242
Betriebsart der lokalen Sicherheitseingänge, 98
Betriebsartenwahlschalter, 111, 150
Betriebsmodus, 182
Bezeichnungen, 18

C

COMM, 21
CONFIGURING (Konfigurieren), 182
Connection Type (Parameter), 70–71
CRITICAL ERROR (Kritischer-Fehler-Zustand), 182

D

DeviceNet-Kommunikationsspezifikationen, 29
DeviceNet-Stecker, 24, 49
Dezentraler E/A-Bereich, 57
Discrepancy Error, 100–101
Diskrepanzzeit, 99, 112, 114
Dual Channel Complementary, 99, 112
Dual Channel Complementary (2 Pairs), 112
Dual Channel Equivalent, 99–100, 112
Dual Channel Equivalent (2 Pairs), 112
Dual Channel Mode (Parameter), 99, 103

E

E/A-Aktualisierungszeit, 191
E/A-Kommentare, 90
E/A-Tags, 57, 77, 80, 90, 99, 104
E/A-Typ, 77, 80
EDM, 111, 152
Ein- und Ausgangsgrößeneinstellungen, 115
Eingangs- und Ausgangsklemmen und interne Verbindungen, 25
Eingangsarteinstellungen, 112
Eingangsausschaltverzögerungen, 98
Eingangseinschaltverzögerung, 98
Eingangs-Tags, 109
Einkanalmodus, 99, 104, 112
Einschaltverzögerung, 111, 149
Einsehen und Löschen der Fehlerprotokolltabelle, 207
Einstellen des Fehlerausgangs (Use Fault Present), 116
Einstellung der Betriebsart, 103
Einstellung der Sendebedingung, 86
Einstellung der Slave-E/A, 80
Einstellung der Triggeradresse, 86
Einstellungen für Sicherheits-E/A-Verbindungen, 70
EPI (Expected Packet Interval), 70
EPI (Expected Packet Interval) (Parameter), 70, 72
Erstellung der zu versendenden Explicit Message, 86
EXNOR, 111
EXOR, 111
Explicit Message-Kommunikation, 83
Externe Relaisüberwachung, 111, 152

F

Fehlerhaltezeit, 101, 105
Fehlerprotokoll, 202
Fehlerprotokollbereich, 207
Fehlerprotokolltabelle, 207
Festlegen der E/A-Tags, 77
Festlegen der zusätzlich zu übertragenden Statusinformationen, 77, 80

Festlegen des E/A-Typs (Parameter „I/O Type“), 77
Festlegen von Funktionsblockparametern, 112
Funktionsblöcke, 111─112
Funktionstests, 115

G

Geringfügige Fehler, 200, 202
Gesamteinschaltdauer-Alarmschwellenwert, 95
Gesamteinschaltdauer-Überwachung, 93
Gesetze und Richtlinien, xix
Glossar, 253

I

IDLE (Leerlauf), 182
Impulsgeber, 172
IN 0 bis 15, 21
IN 0 bis 39, 21
Inspektion, 224

K

Kennwort, 180
Knotenadresseneinstellung, 52
Knotenadressen-Mehrfachverwendungs-Fehler, 52
Knotenadressenschalter, 23
Komparator, 126
Konfiguration der Daten des dezentralen E/A-Bereichs, 59
Konfigurationsschutz, 21, 178
Kritische Fehler, 200, 202

L

LED-Kontrollleuchten, 21
Lichtgitter-Überwachung, 111, 137
LOCK, 21
LOCK (LED-Anzeige), 178
Logik-Funktionen, 108, 111
Lokale Ausgänge, 85
Lokale Ausgangsüberwachung, 67
Lokale Eingänge, 85
Lokale Eingangsüberwachung, 66
Lokale Sicherheits-E/A, 3

M

Mehrfache Verwendung einer Knotenadresse, 23
MS, 21, 55
Multi Connector, 175
Multicast-Verbindung, 71
Muting, 154

N

NE1A-Serie, 3
Netzwerkkonfigurator, 16
Netzwerkreaktionszeit, 192
Netzwerkstatus, 21, 55
nicht sichere Daten, 66, 77
Normales Verhalten bei der Einstellung „Dual Channel Equivalent“, 114
Normen, xix
NOT, 111, 117
NOT-AUS-Taster-Überwachung, 111, 134
NS, 21, 55

O

Online-Überwachung, 6
Open Type (Parameter), 70─71
Operating Mode at Startup (Parameter), 185
OR, 111, 121
OUT 0 bis 7, 21
Output Channel Mode (Parameter), 103

P

Parametrieren von Funktionsblöcken, 112
Programmkapazität, 110

R

Reaktionszeit, 193
Reaktionszeitberechnung, 194
Reset, 111, 129
Restart, 111, 132
Routing, 111, 153
RS-FF, 124
Rücksetzung, 179
Rücksetzvarianten, 179
RUN (Betrieb), 182

S

Schalthäufigkeitszähler, 91
Schaltspielalarm-Schwellenwert, 91
SELF-DIAGNOSTIC (Selbstdiagnose), 182
Sicherheitsausgangsklemmen, 25
Sicherheitsdaten, 64─66, 72
Sicherheits-E/A-Kommunikation, 3, 70
Sicherheitseingang, 98
Sicherheitseingangsklemmen, 25
Sicherheitskette, 193, 198
Sicherheits-Master, 69
Sicherheitsnetzwerk-Controller, 2
Sicherheitssignatur, 71
Sicherheits-Slave, 69, 76
Sicherheits-Slave-E/A, 83
Sicherheitssteuerungssystem, 9─10
Sicherheitstür-Überwachung, 111, 139
Sicherheitsverbindungen, 70
Sicherheitsvorkehrungen, xxi
Siebensegmentanzeige, 22
Singlecast-Verbindung, 71
Slave-E/A, 79─80
Softwareeinstellung, 23, 52
Spannungsversorgungsklemme (+ 24 V DC) für externe Ausgangsgeräte, 25
Spannungsversorgungsklemme (+24 V DC) für externe Eingangsgeräte und Testausgänge, 25
Speichereinstellung für den E/A-Bereich von Slaves, 58
Standalone-Controller, 54
Standalone-Controller-Modus, 3
Standalone-System, 13
Standard-E/A-Kommunikation, 3, 79
Standard-Slave, 79
Status der lokalen Ausgänge, 21, 65, 76─77, 80─81
Status der lokalen Eingänge, 21, 64─65, 76─77, 80─81
Status der Testausgänge/Muting-Lampe, 66, 76─77, 80─81
Synchronisationszeit, 115
Systemkonfiguration, 8

T

Test Source (Parameter), 98
Testausgänge, 85
Testausgänge (Parameter), 102

U

Übersicht über die Programmierung, 108
Überwachung der E/A-Versorgungsspannung, 91
Überwachungssystem, 9─10
Unterstützte Funktionsblöcke, 111
USB-Buchse, 24
USB-Kommunikationsstatus, 21

V

Verlorengegangenes Kennwort, 180
Versorgungsspannung für die internen Schaltkreise, 25
Verteiltes Sicherheitssteuerungssystem, 11

W

Während der Selbstdiagnose festgestellter Fehler, 101, 104
Warten auf TUNID-Einstellung, 183

X

XNOR, 111, 124
XOR, 111, 123

Z

Zähler, 173
Zentralisiertes Überwachungssystem, 11
Zugangsbeschränkung, 180
Zurücksetzen von Fehlern, 101, 105
Zustimmschalter, 170
Zweihandsteuerung, 111, 145
Zweikanalmodus, 99, 104
Zykluszeit, 189

Versionshistorie

Die letzte Zahl der Dokumentennummer in der unteren linken Ecke der Vorder- und Rückseite dieses Bedienerhandbuchs gibt den Überarbeitungsstand an.

Die folgende Tabelle führt die mit den einzelnen Überarbeitungen vorgenommenen Änderungen auf. Die Nummerierung der Seiten bezieht sich auf die vorherige Version.

Versionscode	Datum	Überarbeitung
01	April 2005	Ursprungsversion
02	April 2006	**Seite 16**: Vorschriften und Normen modifiziert. **Seite 34**: Informationen zur Siebensegmentanzeige modifiziert. **Seite 38**: Informationen zu DeviceNet-Kommunikationsspezifikationen hinzugefügt. **Seite 59**: Informationen zum Einstellen von Knotenadressen hinzugefügt. **Seite 60**: Informationen zum Einstellen von Baudraten hinzugefügt. **Seite 63**: Informationen zur Siebensegmentanzeige modifiziert. **Seiten 64 bis 67**: Informationen zur Datenkonfiguration des dezentralen E/A-Bereichs hinzugefügt. **Seite 80**: Informationen zur Übermittlung von Explicit Messages hinzugefügt. **Seiten 88 und 92**: Informationen zum Einstellen der Fehlerhaltezeit hinzugefügt. **Seite 103**: Informationen zum Einstellen der Anzahl von Ein- und Ausgängen geändert. **Seite 103**: Informationen zum Einstellen von Ausgangspunkten geändert. **Seiten 114 und 116**: Überschriften geändert. **Seiten 113, 118, 121, 124 und 128**: Informationen zum Einstellen optionaler Ausgänge geändert. **Seiten 126 und 134**: Informationen zu Fehlerhandhabung und Zurücksetzung hinzugefügt. **Seiten 154 bis 157**: Informationen zur Berechnung von Reaktionszeiten hinzugefügt. **Seite 161**: Informationen zum Kontrollleuchtenstatus hinzugefügt. **Seite 166**: Informationen zur Fehlerprotokolltabelle hinzugefügt. **Seite 167**: Informationen zu Fehlerdatendetails hinzugefügt. **Seiten 169 bis 172**: Informationen zu Korrekturen als Reaktion auf Display-Meldungen geändert und hinzugefügt. **Seiten 173 bis 176**: Informationen zu Verbindungsstatus-Tabellen hinzugefügt. **Seite 184**: Änderungen und Erweiterungen des Glossars.
03	September 2006	Funktionsbeschreibungen der Sicherheitsnetzwerk-Controller NE1A-SCPU01-V1 Ver. 1.0 und NE1A-SCPU02 Ver.1.0 hinzugefügt.